# HP Insight Remote Support

## Guia de Configuração de Dispositivos Monitorados

Versão do software: 7.4

Data de publicação do documento: Julho de 2015

Data de lançamento do software: Julho de 2015

# Informações legais

## Garantia

As únicas garantias para produtos e serviços da HP são as estabelecidas nas declarações de garantia expressa que acompanham tais produtos e serviços. Nenhum item deste documento deve ser interpretado como constituindo garantia adicional. A HP não será responsável por eventuais erros técnicos ou editoriais ou omissões contidos neste documento.

As informações contidas neste documento estão sujeitas a alterações sem notificação.

## Legenda de direitos restritos

Software de computador confidencial. Licença válida da HP exigida para posse, uso ou cópia. Consistente com as normas FAR 12.211 e 12.212, de software para computador comercial, documentação de software de computador e dados técnicos para itens comerciais licenciados ao governo dos Estados Unidos da América por meio de licença comercial padrão.

## Informações sobre direitos autorais



## Avisos de marcas comerciais

Microsoft® e Windows® são marcas comerciais do grupo de empresas Microsoft.

UNIX® é uma marca comercial registrada do The Open Group.

Linux® é marca comercial registrada da Linus Torvalds nos EUA e em outros países.

Red Hat® é marca comercial registrada da Red Hat, Inc. nos Estados Unidos e em outros países.

Citrix® e XenDesktop® são marcas comerciais registradas da Citrix Systems, Inc. e/ou de uma ou mais de suas subsidiárias e podem estar registradas na Agência de Marcas e Patentes dos EUA e de outros países.

Intel®, Itanium® e Intel® Xeon® são marcas comerciais da Intel Corporation nos Estados Unidos e em outros países.

© 2012 Google Inc. Todos os direitos reservados. Chrome™ é marca comercial da Google Inc.

# Conteúdo

# Prefácio

## Objetivo e público-alvo do documento

Este documento fornece as informações necessárias para configurar dispositivos monitorados antes de detectar esses dispositivos com o HP Insight Remote Support (RS).

Este documento destina-se a clientes da HP e ao pessoal de suporte da HP que estejam instalando, configurando e usando o Insight RS.

## Visão geral do produto

O Insight RS é uma solução de software que possibilita um suporte remoto reativo e proativo para melhorar a disponibilidade de servidores, sistemas de armazenamento e outros dispositivos compatíveis no seu datacenter. O Insight RS conta com vários componentes da HP e com a comunicação entre vários aplicativos de software dentro da empresa do cliente e entre esta e a HP para a prestação de serviços de suporte. Os componentes do software podem ser instalados no dispositivo host ou nos dispositivos monitorados, dependendo da finalidade.

O Insight RS pode ser usado isoladamente ou integrado ao HP Systems Insight Manager (SIM).

Para obter mais informações sobre o Insight RS, acesse: http://www.hp.com/go/insightremotesupport.

**Importante:** Para configurar adequadamente o Insight RS, é essencial que você leia este documento na íntegra *antes* de continuar a instalação do Insight RS.

# Documentos relacionados

Para obter documentações adicionais do Insight RS, acesse:
http://www.hp.com/go/insightremotesupport/docs.

- *Notas de Lançamento do HP Insight Remote Support*

  Este documento fornece detalhes do produto e informações sobre quais dispositivos monitorados e dispositivos host podem ser usados com a solução Insight RS.
- *Guia de Instalação Rápida do HP Insight Remote Support*

  Este documento fornece uma lista de verificação para a instalação e a configuração do Insight RS.
- *Guia de Instalação e Configuração do HP Insight Remote Support*

  Este documento fornece informações detalhadas sobre a instalação e a configuração do Insight RS.
- *Guia de Configuração de Dispositivos Monitorados do HP Insight Remote Support*

  Este documento fornece informações para configurar os dispositivos que serão monitorados pelo Insight RS.
- *Informe de Segurança do HP Insight Remote Support*

  Este documento fornece uma visão geral dos recursos de segurança disponíveis no Insight RS.
- *Guia de Atualização do HP Insight Remote Support*

  Este documento fornece informações sobre a atualização do Insight RS para a versão 7.4.
- *Guia de introdução ao HP Insight Online*

  Este documento oferece informações sobre os pré-requisitos de uso do HP Insight Online e explica como utilizar o Insight Online para gerenciar os dispositivos, contratos e garantias HP de sua empresa.

# Histórico de revisões do documento

| Edição | Versão do software | Data de publicação | Resumo de alterações |
|---|---|---|---|
| 1.0 | 7.4 | Julho de 2015 | Versão inicial. |

# Registe-se para receber comunicações do Insight Remote Support

A equipe de produto do HP Insight Remote Support usa o processo de comunicação de suporte da HP para comunicar notícias importantes, como comunicados de engenharia, comunicados para clientes, avisos de engenharia e avisos para clientes.

Para se inscrever e receber comunicações de suporte usando o HP Subscribers Choice, acesse: https://h30046.www3.hp.com/SubChoice/country/us/en/signin.aspx.

Ao se inscrever, procure *Insight Remote Support*.

# Informações de suporte da HP

A HP recomenda que você consulte a documentação do Insight RS para resolver problemas. A documentação foi elaborada para guiá-lo até uma instalação e configuração feita com êxito. No entanto, se for necessário suporte adicional para o Insight RS, você poderá obter ajuda por meio dos Centros de Resposta locais da HP. Para obter detalhes de contato, acesse:http://www.hp.com/go/rstechsupport.

Antes de contatar o suporte, você pode verificar se o seu problema tem uma solução disponível. Um contrato válido e o login no HP Passaporte são necessários para visualizar documentos de solução de problemas.

Para visualizar soluções de problemas do Insight RS, conclua as seguintes etapas:

1. Acesse http://www.hp.com e navegue até **Suporte** → **Suporte e solução de problemas**.
2. No campo **Procure por produto**, digite `Insight Remote Support` e clique em **Continue**.
3. Nos resultados da pesquisa, clique em **Software HP Insight Remote Support de última geração**.
4. No painel **Soluções mais visualizadas**, clique em **Visualizar tudo** para ver as soluções.

# Agradecemos os seus comentários!

Se você tem comentários sobre este documento, entre em contato com a equipe de documentação por e-mail. Se um cliente de e-mail estiver configurado neste sistema, clique no link acima para abrir uma janela de e-mail com as seguintes informações na linha de assunto:

**Comentários sobre o Guia de Configuração de Dispositivos Monitorados do Insight Remote Support 7.4**

Basta adicionar seus comentário ao e-mail e clicar em Enviar.

Se nenhum cliente de e-mail estiver disponível, copie as informações acima em uma nova mensagem de algum cliente de e-mail na web e envie seus comentários para techdocs_feedback@hp.com.

# Capítulo 1: Noções básicas dos pré-requisitos para dispositivos monitorados

Para usar o Insight Remote Support (RS), é preciso ter pelo menos dois equipamentos: um servidor ProLiant compatível com Windows para ser usado como o dispositivo host, e um ou mais dispositivos a serem monitorados pelo Insight RS. Consulte a tabela abaixo para identificar quais protocolos e componentes de software são necessários para seus dispositivos monitorados, depois consulte o capítulo específico referente a seus dispositivos para concluir os detalhes de configuração. Antes de começar, verifique se o Insight RS oferece suporte aos dispositivos monitorados, consultando o *Notas de Lançamento do HP Insight Remote Support*.

O Insight RS verifica a garantia e o contrato de todos os dispositivos para certificar-se de que eles possuem uma garantia, Care Pack ou contrato HP válido. Se um dispositivo não tiver uma garantia ou contrato HP, o indicador de integridade de monitoramento no Insight RS Console aparecerá em vermelho. O indicador vermelho significa que eventos de serviço não serão analisados ou enviados à HP.

## Identificar componentes de software e protocolos de comunicação necessários

Os dispositivos monitorados conseguem se comunicar com o dispositivo host usando um ou mais dos seguintes protocolos de comunicação e componentes de software:

- Event Log Monitoring Collector (ELMC)
- HP P6000 Command View
- Hypertext Transfer Protocol Secure (https)
- Hypertext Transport Protocol (http)
- iLO Remote Insight Board Command Language Protocol (RIBCL)
- Solução SAN P4000 (SAN/iQ)
- Secure Shell (SSH)
- Simple Network Management Protocol versão 1 (SNMPv1)
- Simple Network Management Protocol versão 2 (SNMPv2)
- Simple Network Management Protocol versão 3 (SNMPv3)

**Observação:** O HP Insight RS oferece suporte ao protocolo SNMPv3 seguro quando este é compatível no dispositivo monitorado. Consulte a documentação do seu dispositivo para determinar as versões do SNMP com suporte no seu dispositivo.

- Telnet
- Interface do serviço web do VMware VirtualCenter
- Protocolo de gerenciamento dos serviços Web (WS-Man)
- Web-Based Enterprise Management (WBEM)
- Windows Management Instrumentation (WMI)

Se você não configurar os protocolos e softwares necessários para seus dispositivos monitorados, os dispositivos *não* irão se comunicar com o dispositivo host e a coleta de seus eventos e configurações *não* será enviada à HP para suporte.

**Importante:** Você precisa não só configurar o protocolo no dispositivo monitorado, mas também acrescentar o protocolo dentro do Console do Insight RS para que o Insight Remote Support possa acessar o dispositivo.

**Importante:** Se você alterar o nome de usuário/senha que o Insight RS usa para conectar os dispositivos monitorados, ou se as credenciais expirarem como parte das políticas de segurança, você *deve* modificar essas credenciais correspondentes no Console do Insight RS para continuar monitorando os dispositivos.

**Importante:** Insight RS requer acesso de administrador aos dispositivos monitorados. Descobertas e coleções exigem acesso privilegiado para recuperarem informações sobre os dispositivos monitorados.

Os protocolos e softwares necessários são determinados pelo tipo de dispositivo monitorado. Leia o capítulo deste documento correspondente ao dispositivo monitorado para entender que configuração é necessária para seu dispositivo monitorado específico. Alguns tipos de dispositivo monitorado podem usar vários protocolos de comunicação. O protocolo que você escolhe depende de suas preferências e estratégia de segurança.

Em alguns casos, é preciso usar mais de um protocolo. Alguns protocolos podem ser usados pelo Insight RS Console para detectar dispositivos monitorados, enquanto outros protocolos podem ser usados para monitorar eventos de hardware ou recuperar informações de coleta de configurações dos dispositivos monitorados. A tabela a seguir destaca os requisitos, mas leia a seção referente a seu tipo de dispositivo monitorado, para mais detalhes.

**Atribua dispositivos às coletas de SAN na guia Serviços de coleta** → Agendamento de coletas do Insight RS Console, no Agendamento de coleta de configuração SAN. Consulte a Ajuda para obter mais informações sobre como configurar suas coletas de SAN.

**Tabela 1.1** ***Protocolos de comunicação e componentes necessários para dispositivos monitorados para o Insight RS***

| | Detecção | Monitoramento | Coletas básicas | Coletas de SAN | Observações |
|---|---|---|---|---|---|
| **Servidores HP** | | | | | |
| ProLiant Gen8 e Gen9 | RIBCL | RIBCL | RIBCL | | Servidores HP ProLiant Gen8 e Gen9 podem ser monitorados com o uso da funcionalidade incorporada do Remote Support disponível no iLO 4 e no Intelligent Provisioning ou com o uso de um agente de diagnóstico instalado no sistema operacional.<br>Observação: se você quiser monitorar dispositivos anexados, será necessário instalar o HP Service Pack for ProLiant, conforme detalhado na seção do servidor ProLiant que corresponde ao sistema operacional abaixo.<br>Credenciais do protocolo RIBCL são necessárias por todos os servidores HP ProLiant Gen8 e Gen9, independentemente do uso dos recursos incorporados ou do agente de diagnóstico.<br>Consulte "Configurar servidores ProLiant Gen8 e Gen9". |
| Windows no ProLiant | SNMP ou WMI | SNMP ou WMI | SNMP ou WMI | | É preciso instalar o HP Service Pack for ProLiant e todos os provedores que o acompanham.<br>Você pode optar por usar o SNMPv1 ou o WMI. Porém, para reunir Coletas de SAN para um servidor Windows ProLiant, é necessário usar o WMI. O Insight RS requer os Provedores WBEM do Insight Management versão 2.8 ou posterior, mas a HP recomenda a instalação da versão mais recente disponível para o seu dispositivo.<br>Consulte "Configurar servidores ProLiant Windows".<br>Para configurar usando o WMI, consulte "Configurar servidores ProLiant Windows usando o WMI".<br>Para configurar usando o SNMP, consulte "Configurar servidores ProLiant Windows usando o SNMP". |
| | | | | WMI | |

**Tabela 1.1** ***Protocolos de comunicação e componentes necessários para dispositivos monitorados para o Insight RS, continuação***

| | Detecção | Monitoramento | Coletas básicas | Coletas de SAN | Observações |
|---|---|---|---|---|---|
| Linux no ProLiant | SNMP | SNMP | SNMP | | É preciso instalar o HP Service Pack for ProLiant e todos os provedores que o acompanham.<br>Consulte "Configurar servidores ProLiant Linux". |
| | | | | Telnet ou SSH | |
| VMware® ESX® no ProLiant | SNMP | SNMP | SNMP | | Consulte "Configurar servidores ProLiant VMware ESX". |
| | | | | SSH | |
| VMware® ESXi™ no ProLiant | WBEM | WBEM | WBEM | WBEM | Consulte "Configurar servidores ProLiant VMware ESXi". |
| Servidor Citrix Xen no ProLiant | SNMP | SNMP | SNMP | | Consulte "Configurar ProLiant Citrix XenServers". |
| | | | | Telnet ou SSH | |
| Hyper-V Server no ProLiant | SNMP ou WMI | SNMP ou WMI | | | Não há suporte para coletas de configuração.<br>Para monitoramento, siga as instruções de configuração para um servidor ProLiant Windows.<br>Consulte "Configurar servidores ProLiant Windows". |
| Windows 2003 no Integrity | WMI | WMI | WMI | WMI | É preciso instalar o Integrity Support Pack e todos os provedores que o acompanham. Ele inclui a instalação do SNMP e do WMI.<br>Consulte "Configurar servidores Integrity Windows 2003". |
| | SNMP | SNMP | SNMP | | |
| | | ELMC | | | |
| Windows 2008 no Integrity | WMI | WMI | WMI | WMI | É preciso instalar o HP Integrity Support Pack e todos os provedores que o acompanham.<br>Consulte "Configurar servidores Integrity Windows 2008". |
| Linux no Integrity | WBEM | WBEM | | | Coletas de configuração não têm suporte, exceto quando o servidor faz parte de uma coleta de SAN. Você pode optar por usar tanto o Telnet quanto o SSH para reunir coletas de SAN de um servidor Integrity Linux.<br>Consulte "Configurar servidores Integrity Linux". |
| | | | | Telnet ou SSH | |

**Tabela 1.1** ***Protocolos de comunicação e componentes necessários para dispositivos monitorados para o Insight RS, continuação***

| | Detecção | Monitoramento | Coletas básicas | Coletas de SAN | Observações |
|---|---|---|---|---|---|
| HP-UX no Integrity | WBEM | WBEM | WBEM | | Instale os WBEM Providers apropriados no HP-UX. Em geral, eles fazem parte do conjunto de recursos do HP-UX e são atualizados por meio de correções e softwares no dispositivo, conforme o caso. |
| | | | | Telnet ou SSH | Você pode optar por usar tanto o Telnet quanto o SSH para reunir coletas de SAN para um servidor Integrity HP-UX.<br>Consulte "Configurar servidores Integrity HP-UX". |
| Onboard Administrator (OA) do HP Integrity Superdome 2 | WS-Man | WS-Man | WS-Man | | A detecção e as coletas usam o WS-Man. O OA é monitorado através do WS-Man, mas as partições do Superdome 2 são monitoradas através do WBEM.<br>Consulte "Configurar servidores Integrity Superdome 2". |
| Onboard Administrator (OA) do HP Integrity Superdome X | WS-Man | WS-Man | WS-Man | | As partições são monitoradas por meio do OA usando o WS-Man.<br>Para coletas, o Insight RS se comunica diretamente com a partição. Partições Linux se comunicam usando WS-Man. Partições Windows se comunicam usando WinRM.<br>Consulte "Configurar servidores Integrity Superdome X". |
| OpenVMS no Integrity | WBEM | | WBEM | | É preciso instalar o OpenVMS WBEM Provider.<br>A detecção e a coleta de configurações só funcionam quando os WBEM Providers são instalados e as credenciais são devidamente configuradas.<br>Consulte "Configurar servidores OpenVMS". |
| | | ELMC | | | |
| | | | | Telnet ou SSH | |
| OpenVMS no AlphaServer | SNMP | | | | Coletas de configuração não têm suporte, exceto quando o servidor OpenVMS faz parte de uma coleta de SAN.<br>Consulte "Configurar servidores OpenVMS" e a observação especial sobre o suporte para esta plataforma. |
| | | ELMC | | | |
| | | | | Telnet | |

**Tabela 1.1** ***Protocolos de comunicação e componentes necessários para dispositivos monitorados para o Insight RS, continuação***

| | Detecção | Monitoramento | Coletas básicas | Coletas de SAN | Observações |
|---|---|---|---|---|---|
| Tru64 UNIX no AlphaServer | SNMP | | | | Coletas de configuração não têm suporte, exceto quando o servidor Tru64 faz parte de uma coleta de SAN.<br>Você pode optar por usar tanto o Telnet quanto o SSH para reunir coletas de SAN para um servidor Tru64 Linux.<br>Consulte "Configurar servidores Tru64 UNIX" e a observação especial sobre o suporte para esta plataforma. |
| | | ELMC | | | |
| | | | | Telnet ou SSH | |
| Sistemas de mensagens E5000 | SNMP ou WMI | SNMP ou WMI | SNMP ou WMI | | Esses dispositivos devem ser configurados da mesma forma que um servidor ProLiant Windows.<br>Você pode optar por usar o SNMP ou o WMI. Porém, para reunir Coletas de SAN, é necessário usar o WMI.<br>As coletas de configuração para o conector de chassi usam HTTP.<br>Consulte "Configurar servidores ProLiant Windows". |
| | | | | WMI | |
| | | | HTTP | | |
| Sistemas HP NonStop | (Consulte as notas) | | | | Para obter mais detalhes sobre como instalar e configurar o Insight RS para uso em um ambiente NonStop, consulte o documento *Insight Remote Support para NonStop*, disponível em www.hp.com/go/nonstop-serviceinfo. |
| **Servidores Non-HP** | | | | | |
| Windows em servidores IBM | SNMP | SNMP | | | Não há suporte para coletas de configuração.<br>Consulte "Configurar servidores IBM". |
| Windows no Dell PowerEdge | SNMP | SNMP | | | Não há suporte para coletas de configuração.<br>Consulte "Configurar servidores Dell PowerEdge". |

**Tabela 1.1** ***Protocolos de comunicação e componentes necessários para dispositivos monitorados para o Insight RS, continuação***

| | Detecção | Monitoramento | Coletas básicas | Coletas de SAN | Observações |
|---|---|---|---|---|---|
| **HP BladeSystems** | | | | | |
| HP Onboard Administrator para gabinetes classe C | SNMP | SNMP | | | Os gabinetes HP BladeSystem classe C podem ser monitorados com o uso de recursos de gerenciamento incorporados no HP Onboard Administrator (OA) ou por meio da configuração do SNMP no OA.<br>Consulte "Configurar gabinetes BladeSystem classe C".<br>Para configurar o OA, consulte "Configurar gabinetes BladeSystem classe C com o OA".<br>Para configurar usando o SNMP, consulte "Configurar gabinetes BladeSystem classe C usando SNMP". |
| | | | HTTPS | | |
| Servidores HP ProLiant BladeSystem | (Consulte as notas) | | | | Os servidores ProLiant BladeSystem com suporte são monitorados independentemente do gabinete classe C em que estão instalados. Os servidores ProLiant BladeSystem podem ser configurados seguindo-se as instruções para servidores ProLiant.<br>Para detalhes de configuração, consulte a seção do servidor ProLiant que corresponde ao sistema operacional instalado no servidor ProLiant BladeSystem. |
| Servidores HP Integrity BladeSystem | (Consulte as notas) | | | | Os servidores Integrity BladeSystem com suporte são monitorados independentemente do gabinete classe C em que estão instalados. Os servidores Integrity BladeSystem podem ser configurados seguindo-se as instruções para servidores Integrity.<br>Para detalhes de configuração, consulte a seção do servidor Integrity que corresponde ao sistema operacional instalado no servidor Integrity BladeSystem. |

**Tabela 1.1** ***Protocolos de comunicação e componentes necessários para dispositivos monitorados para o Insight RS, continuação***

| | Detecção | Monitoramento | Coletas básicas | Coletas de SAN | Observações |
|---|---|---|---|---|---|
| Blades de armazenamento | (Consulte as notas) | | | | Não há suporte para coletas de configuração.<br>Os blades de armazenamento são monitorados através dos agentes de armazenamento instalados no blade de servidor do parceiro. O blade de servidor de parceiro é o blade de servidor adjacente conectado diretamente ao blade de armazenamento. |
| Blades de fita | (Consulte as notas) | | | | Não há suporte para coletas de configuração.<br>Os blades de fita são monitorados através dos agentes de armazenamento instalados no blade de servidor do parceiro. O blade de servidor de parceiro é o blade de servidor adjacente conectado diretamente ao blade de fita. |
| Módulos do Virtual Connect | SNMP | SNMP | SNMP | SNMP | Consulte "Configurar módulos Virtual Connect". |
| **HP Disk Arrays** | | | | | |
| SBM de P6000 Enterprise Virtual Arrays | HP P6000 Command View | HP P6000 Command View | HP P6000 Command View | HP P6000 Command View | Para configurar com o Gerenciamento baseado em servidor, consulte "Configurar Enterprise Virtual Arrays e P6000 com o gerenciamento baseado em servidor". |
| | | ELMC | | | |
| ABM de P6000 Enterprise Virtual Arrays | HP P6000 Command View | HP P6000 Command View | HP P6000 Command View | HP P6000 Command View | Para configurar com o gerenciamento baseado em array, consulte "Configurar Enterprise Virtual Arrays e P6000 com o gerenciamento baseado em array". |
| HP StoreVirtual 4xxx (anteriormente Soluções SAN P4000 SAN/Armazenamento LeftHand) | SNMP | SNMP | | | Consulte "Configurar sistemas de armazenamento StoreVirtual P4000". |
| | | LeftHand OS | LeftHand OS | LeftHand OS | |

**Tabela 1.1** ***Protocolos de comunicação e componentes necessários para dispositivos monitorados para o Insight RS, continuação***

| | Detecção | Monitoramento | Coletas básicas | Coletas de SAN | Observações |
|---|---|---|---|---|---|
| MSA 1040<br>MSA 2040 | SNMP | SNMP | | | Tanto o SNMP quanto o WBEM devem ser instalados e configurados. |
| | WBEM | WBEM | WBEM | WBEM | Consulte "Configurar Modular Smart Arrays P2000 G3, MSA 1040 e MSA 2040". |
| HP P2000 G3 MSA | SNMP | SNMP | | | Tanto o SNMP quanto o WBEM devem ser instalados e configurados. |
| | WBEM | WBEM | WBEM | WBEM | Consulte "Configurar Modular Smart Arrays P2000 G3, MSA 1040 e MSA 2040". |
| HP MSA23xx G2 | SNMP | SNMP | | | Instale o WBEM SMI-S Proxy Provider no servidor host, e não no MSA propriamente dito. |
| | WBEM | | WBEM | WBEM | Consulte "Configurar Modular Smart Arrays MSA23xx G2". |
| HP MSA2xxx G1 | SNMP | SNMP | | SNMP | Não há suporte para coletas de configuração, exceto quando o MSA2xxx G1 faz parte de uma coleta de SAN.<br>Consulte "Configurar Modular Smart Arrays MSA2xxx G1". |
| HP MSA15xx | SNMP | SNMP | SNMP | SNMP | Consulte "Configurar Modular Smart Arrays MSA15xx". |
| StoreEasy Storage | WMI | WMI | WMI | WMI | Consulte "Configurar sistemas StoreEasy Storage". |
| HP StoreAll Network Storage Systems (o antigo HP IBRIX Storage) | SNMP | SNMP | SNMP | | Consulte "Configurar sistemas StoreAll Storage". |
| HP XP/P9000 | (Consulte as notas) | | | | Para conhecer os modelos com suporte, consulte *Notas de Lançamento do HP Insight Remote Support*.<br>O registo com o Insight RS ocorre durante a configuração do Truststore no SVP. Observe que dispositivos XP/P9000 não são aproveitáveis pelos clientes. O suporte para dispositivos XP/P9000 é fornecido como parte do seu contrato de suporte Mission Critical. Entre em contato com o seu representante de conta local da HP para ajudar a implementar essa solução. |

**Tabela 1.1** ***Protocolos de comunicação e componentes necessários para dispositivos monitorados para o Insight RS, continuação***

| | Detecção | Monitoramento | Coletas básicas | Coletas de SAN | Observações |
|---|---|---|---|---|---|
| **Proteção de dados** | | | | | |
| HP StoreOnce Backup (D2D) | SNMP | SNMP | | | Não há suporte para coletas de configuração.<br>Consulte "Configurar sistemas de backup StoreOnce (D2D)". |
| HP Virtual Library System (VLS) | SNMP | SNMP | | | Coletas de configuração não têm suporte, exceto quando o VLS fa parte de uma coleta de SAN.<br>Consulte "Configurar sistemas de biblioteca virtual". |
| | | | | SSH | |
| HP StoreEver MSL (anteriormente biblioteca de sistemas modulares) | SNMP | SNMP | SNMP | | Consulte "Configurar bibliotecas de fita StoreEver". |
| HP StoreEver ESL (a antiga Enterprise Systems Library) | SNMP | SNMP | | | O WBEM é fornecido por meio do Command View para bibliotecas de fita, instalado no servidor que gerencia as bibliotecas de fita.<br>Consulte "Configurar bibliotecas de fita StoreEver". |
| | | | WBEM | | |
| | | | | Telnet ou SSH | |
| HP StoreEver EML (anteriormente biblioteca modular corporativa) | SNMP | SNMP | | | O WBEM é fornecido por meio do Command View para bibliotecas de fita, instalado no servidor que gerencia as bibliotecas de fita.<br>Consulte "Configurar bibliotecas de fita StoreEver". |
| | | | WBEM | | |
| | | | | Telnet ou SSH | |
| **Comutadores SAN HP StoreFabric** | | | | | |
| Comutador SAN série B | SNMP | SNMP | | | Consulte "Configurar comutadores StoreFabric série B". |
| | | | Telnet ou SSH | Telnet ou SSH | |
| Comutador SAN série C | SNMP | SNMP | SNMP | SNMP | Consulte "Configurar comutadores StoreFabric série C". |

**Tabela 1.1** ***Protocolos de comunicação e componentes necessários para dispositivos monitorados para o Insight RS, continuação***

| | Detecção | Monitoramento | Coletas básicas | Coletas de SAN | Observações |
|---|---|---|---|---|---|
| Comutador SAN série H | SNMP | SNMP | SNMP | SNMP | Consulte "Configurar comutadores StoreFabric série H". |
| **Roteadores e comutadores de rede HP** | | | | | |
| Comutadores baseados no HP ProVision (anteriormente denominados série E/ProCurve) | SNMP | SNMP | | | Consulte "Configurar comutadores de rede baseados no ProVision". |
| | | | Telnet ou SSH | | |
| Comutadores baseados no HP ComWare (anteriormente série A ou H3C/3Com) | SNMP | SNMP | | | Consulte "Configurar comutadores de rede baseados no Comware". |
| | | | Telnet ou SSH | | |
| Switches Mellanox InfiniBand | SNMP | SNMP | SNMP | SNMP | Consulte "Configurar comutadores Mellanox InfiniBand". |
| Roteadores de rede HP | SNMP | SNMP | | | Consulte "Configurar roteadores de rede". |
| | | | Telnet ou SSH | | |
| **Rack e energia** | | | | | |
| UPS de torre e montável em rack da HP | SNMP | SNMP | | | Não há suporte para coletas de configuração.<br>Se o seu UPS usa um Módulo de gerenciamento, consulte "Configurando módulos de gerenciamento UPS".<br>Se o seu UPS usa um Módulo de rede, consulte "Configurando módulos de rede UPS". |

**Tabela 1.1** ***Protocolos de comunicação e componentes necessários para dispositivos monitorados para o Insight RS, continuação***

| | Detecção | Monitoramento | Coletas básicas | Coletas de SAN | Observações |
|---|---|---|---|---|---|
| **Aplicações** | | | | | |
| Servidor VMware® vCenter™ no ProLiant | Interface do serviço web do VMware VirtualCenter | | Interface do serviço web do VMware VirtualCenter | | Reúne coletas de configuração em máquinas virtuais ESX e ESXi, no cluster do VMware vCenter.<br>Consulte "Configurar servidores VMware vCenter". |

# Funcionalidade sem suporte no Insight RS 7.4

Os seguintes dispositivos e recursos eram suportados nas versões 5.x do Insight RS, mas não são na versão 7.4:

**Tabela 1.2 *Funcionalidade do Insight RS 5.x não disponível no Insight RS 7.4***

| Funcionalidade | Detalhes |
|---|---|
| Dispositivo host | • Todas as versões do sistema operacional Microsoft Windows 2003 *não* terão suporte em qualquer versão 7.x do Insight RS. |
| Produtos que *não* serão suportados por nenhuma versão 7.x | • HP Enterprise Secure Key Manager<br>• HP Secure Key Manager<br>• HP Dynamic Smart Cooling<br>• HP SAN Virtualization Services Platform<br>• HP Modular Array<br>• HP Enterprise Modular Array<br>• HP Raid Array<br>• HP Enterprise Storage Array<br>• Comutadores série M (McData)<br>• Servidores com grau de operadora (cx2620, cc3310)<br>• Servidores HP 9000 série rp2400 (Classe A), série rp5400 (Classe L) e D,K,R,T,V (Classe)<br>• Servidores IBM AIX<br>• Servidores Sun Solaris |
| Distribuição de serviços de missão crítica (somente no Insight RSA) | Capacidades para entregar serviços de missão crítica, como:<br>• Avaliações de Verificação de Integridade do Sistema HP-UX (não disponíveis no Insight RS 7.x, mas como um cliente autônomo)<br>• Serviços TAM-S e CCMon<br>• Notificação de dispositivo inacessível |

# Capítulo 2: Configurar servidores ProLiant Gen8 e Gen9

O recurso HP Insight Remote Support (RS), disponível na interface da Web do iLO 4, oferece diagnóstico inteligente de eventos e envio seguro e automático de notificações de eventos para a HP e para o Parceiro distribuidor autorizado da HP por meio da instalação do Insight RS no dispositivo host.

**Importante:** Se você não quiser usar o recurso Remote Support disponível na interface da web do iLO 4, precisará configurar o servidor ProLiant usando agentes SNMP e provedores WBEM. Consulte as informações que correspondem ao seu sistema operacional e siga as instruções de configuração (consulte "Noções básicas dos pré-requisitos para dispositivos monitorados"). Se você usar agentes SNMP ou provedores WBEM, ainda deverá adicionar credenciais de protocolo RIBCL no Insight RS Console. O RIBCL é necessário para que coletas AHS e o Insight RS possam monitorar o servidor.

Para mais informações sobre servidores ProLiant Gen8, acesse:
http://www.hp.com/go/proliantgen8/docs.

# Atender aos requisitos de configuração

Para configurar seus servidores ProLiant Gen8 e Gen9 de forma que eles sejam monitorados pelo Insight RS, conclua as seguintes seções:

**Tabela 2.1** ***Etapas de configuração do ProLiant Gen8 e Gen9***

| Tarefa | Necessário/ Opcional | Concluída? |
|---|---|---|
| Certifique-se de que o Insight RS suporte seu servidor ProLiant, verificando o *Notas de Lançamento do HP Insight Remote Support*. | Necessário | |
| Verifique se o sistema operacional no servidor ProLiant Gen8 está em execução. | Necessário | |
| Instale e configure o Agentless Management Service (AMS) no servidor ProLiant se quiser que o nome de host ou o endereço IP sejam exibidos no lugar do número de série do dispositivo. Para obter mais informações, consulte o problema conhecido "Endereço IP faltando durante a detecção". | Opcional | |

**Tabela 2.1** ***Etapas de configuração do ProLiant Gen8 e Gen9, continuação***

| Tarefa | Necessário/ Opcional | Concluída? |
| --- | --- | --- |
| Verifique se uma versão com suporte do firmware do iLO está instalada no seu servidor ProLiant:<br>• Para servidores HP ProLiant Gen8: A versão 1.10 ou posterior é necessária.<br>• Para servidores HP ProLiant Gen9: A versão 2.00 ou posterior é necessária.<br>**Importante:** Para solucionar vulnerabilidades de softwares de terceiros, a HP recomenda o uso do iLO 4 2.03 ou versão posterior. Para acessar a interface Web do iLO 4 2.03 ou versão posterior, você deve habilitar o TLS no seu navegador. O TLS é o sucessor do SSL (Secure Sockets Layer).<br>Você pode baixar o firmware mais recente no site da HP: www.hp.com/support/ilo4. | Necessário | |
| Adicione o protocolo RIBCL ao Insight RS Console. | Necessário | |
| Detecte o servidor ProLiant no Insight RS Console. | Necessário | |
| Envie um evento de teste para verificar a conectividade entre seu servidor ProLiant e o Insight RS. | Necessário | |

# Configurar dispositivos monitorados

Para configurar seus dispositivos monitorados, conclua a seguinte seção:

## Definir configurações de firewall e porta

Para obter uma lista completa de requisitos de firewall e de porta para dispositivos monitorados, consulte o *Informe de Segurança do HP Insight Remote Support*, em: http://www.hp.com/go/insightremotesupport/docs.

# Adicionar credenciais de protocolo e iniciar a detecção

Para detectar seus dispositivos monitorados, conclua as seguintes seções:

## Criar uma credencial de protocolo RIBCL no Insight RS Console

Para permitir que o Insight RS reúna coletas do Active Health Service, você deve configurar as credenciais de protocolo da RIBCL (iLO Remote Insight Board Command Language) no Insight RS Console.

Para configurar o RIBCL no Insight RS Console, conclua as seguintes etapas:

1. Em um navegador da Web, faça logon no Insight RS Console.
2. No menu principal, selecione **Detecção** e clique na guia **Credenciais**.
3. Na lista suspensa **Selecionar e configurar protocolo**, selecione **iLO Remote Insight Board Command Language Protocol (RIBCL)**.
4. Clique em **Novo**. A caixa de diálogo Nova credencial é exibida.
5. Preencha os campos obrigatórios. Use o nome de usuário e senha da interface da web do iLO 4 no servidor ProLiant Gen8.
6. Clique em **Adicionar**.

Adicione uma credencial de protocolo RIBCL para cada nome de usuário e senha exclusivos nos seus servidores ProLiant Gen8.

O Insight RS cria a credencial de protocolo, que é exibida na tabela de credenciais.

# Definir sub-redes de descoberta, se desejar

Ao descobrir um iLO 4 que possui vários endereços IP de servidor, o comportamento padrão do Insight RS é selecionar um dos endereços IP disponíveis com base nas seguintes preferências: `"10.0.0.0/8,172.16.0.0/12,192.168.0.0/16,169.254.0.0/16,0.0.0.0/0"` em que `0.0.0.0/0` representa um intervalo de IP não participar e a rede `10.` tem a maior preferência. Se existirem vários endereços IP em qualquer uma das sub-redes, o comportamento de seleção dentro desse sub-rede será aleatório.

Foi adicionado um comando de configuração para permitir que você redefina essa ordem de preferência e a especifique de forma mais discreta. O comando possui o seguinte formato:

```
rsadmin config –set siteipv4subnet.preference=<ipv4>/<prefixo>[,<ipv4>/<prefixo>…]
```

em que uma preferência de sub-rede múltipla pode ser definida.

Você pode usar o comando definir uma sub-rede IPv4 preferencial mais discreta, por exemplo: `10.2.x.x` a `10.1.x.x`.

Exemplo:

```
rsadmin config –set siteipv4subnet.preference=10,2.0,0.0/16
```

Você pode preferir a sub-rede `192,168.x.x` a todas as outras.

Exemplo:

```
rsadmin config –set siteipv4subnet.preference=192,168.0,0.0/16
```

Você também pode definir duas ou mais preferências.

Exemplo:

```
rsadmin config –set siteipv4subnet.preference=10.2.0.0/16,10.1.0.0/16
```

Se o dispositivo não for acessível na sub-rede preferencial, o Insight RS continuará a pesquisar a lista de preferências. Por exemplo, se o iLO mostrar uma rede `10.` e o Insight RS não tiver uma conexão `10.`, o Insight RS continuará a pesquisar.

# Detectar o servidor ProLiant Gen8 ou Gen9

Habilite o servidor ProLiant Gen8 ou Gen9 para o Insight Remote Support de uma destas duas maneiras:

- Detecte o servidor ProLiant no Insight RS Console.

  Consulte "Detectar o servidor ProLiant RS por meio do Insight RS Console".
- Registre o Remote Support na interface da Web do iLO 4 do servidor ProLiant.

  Consulte "Ativar o Insight Remote Support para um servidor ProLiant".

**Observação:** Você também pode se registrar para suporte remoto através da interface de provisionamento inteligente. Para obter mais informações, consulte o *Guia de Configuração do HP Insight Remote Support e do Insight Online para servidores ProLiant e gabinetes BladeSystem classe C*, em: http://www.hp.com/go/insightremotesupport/docs.

## *Detectar o servidor ProLiant RS por meio do Insight RS Console*

Para detectar o servidor ProLiant por meio do Insight RS Console, conclua as seguintes etapas:

1. Em um navegador da Web, faça logon no Insight RS Console.
2. No menu principal, selecione **Detecção** e clique na guia **Fontes**.
3. Expanda a seção Endereços IP e adicione o endereço IP do seu dispositivo:
   a. Clique em **Novo**.
   b. Selecione **Endereço único**, **Intervalo de endereços** ou **Lista de endereços**.
   c. Digite os endereços IP dos dispositivos a serem detectados. Use o endereço IP do iLO.
   d. Clique em **Adicionar**.
4. Clique em **Iniciar detecção**.

**Observação:** Após a detecção, o sistema operacional do servidor ProLiant não aparecerá no Insight RS Console. Isso é normal.

## *Ativar o Insight Remote Support para um servidor ProLiant*

Com o Mecanismo de gerenciamento HP iLO, não é preciso instalar nenhum protocolo extra no servidor ProLiant. Você só precisa registrar o servidor ProLiant no dispositivo host para habilitar o Insight Remote Support. Você pode registrar o Insight Remote Support para um servidor ProLiant na interface Web do iLO 4.

**Importante:** Quando for configurar a interface da web do iLO 4, é importante definir o fuso horário. Se o fuso horário não for definido, os eventos enviados para o Insight Remote Support serão exibidos com uma diferença de fuso horário do GMT. Na interface da Web do iLO 4, navegue até **Administração** → **Rede** → **Configurações de SNTP** para definir seu fuso horário.

**Use a tela Remote Support** → Registro para registrar e ativar o Remote Support. Você precisa ter privilégio de configuração do iLO para modificar as configurações do Remote Support.

Para habilitar um servidor ProLiant para o Insight Remote Support, conclua as seguintes etapas:

1. Faça logon na interface da Web do iLO4 (`https://`*`<nome de host ou endereço IP do iLO>`*).
2. No menu de navegação, clique em **Remote Support** → **Registro**. Aparece a tela Registrar e habilitar suporte automatizado.
3. Preencha o campo Nome do host ou endereço de IP.
4. No campo Porta, digite `7906`.
5. Clique em **Registrar**. A interface da Web do iLO 4 registra o dispositivo, e aparece uma mensagem de confirmação.

**Observação:** Após o registro, você poderá ver tanto o servidor ProLiant quanto a interface da Web do iLO 4 listados no Insight RS Console. A interface da Web do iLO 4 desaparecerá se as credenciais do servidor ProLiant e do RIBCL tiverem sido configuradas corretamente.

**Observação:** Após a detecção, o sistema operacional do servidor ProLiant não aparecerá no Insight RS Console. Isso é normal.

# Testar a comunicação do servidor ProLiant Gen8 ou Gen9 com o Insight RS

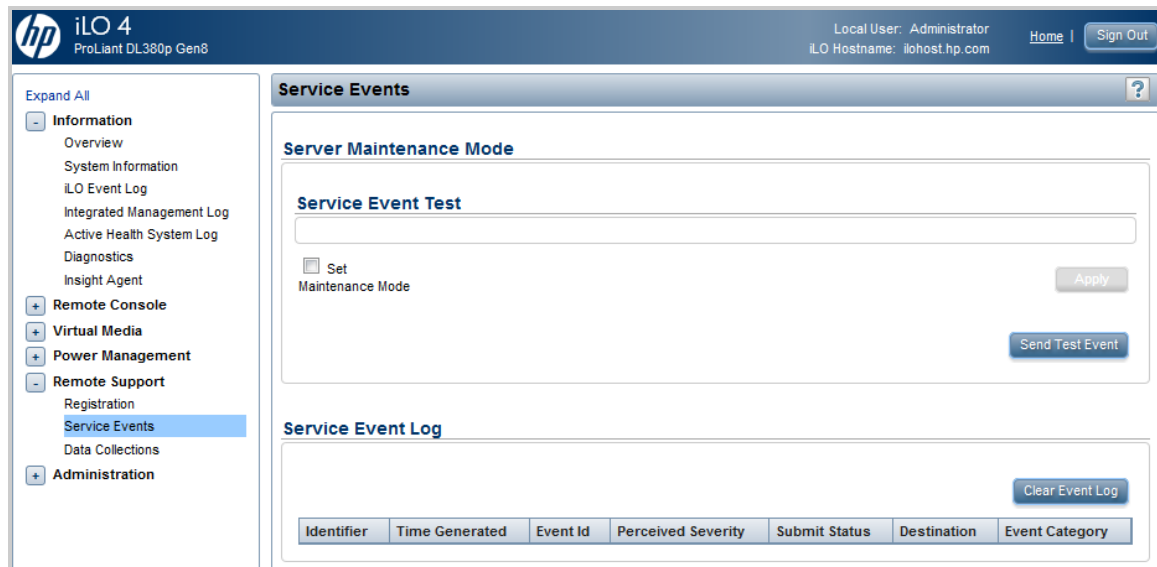
Para verificar a comunicação entre o dispositivo monitorado e o Insight RS, conclua as seguintes seções:

## Verificar o monitoramento de eventos de serviço

Depois de registrar o servidor ProLiant no Insight Remote Support, envie um evento de teste para confirmar a conexão.

**Observação: O envio de interceptações de testes SNMP na página da interface Web do iLO 4** Administração → Gerenciamento não tem suporte suportado no Insight Remote Support. Para enviar um evento de teste, use a página **Remote Support** → **Eventos de serviço**, conforme mostrado abaixo.

Para enviar um evento de teste, siga estas etapas:

1. Faça logon na interface da Web do iLO4 (`https://`*<nome de host ou endereço IP do iLO>*).
2. No menu de navegação, clique em **Remote Support** → **Eventos de serviço**. Aparece a tela Eventos de serviço.

3. Clique em **Enviar evento de teste**. A seguinte mensagem aparece:

   `Tem certeza de que deseja enviar um evento de teste?`

4. Clique em **OK** para confirmar se deseja enviar um evento de teste. A seguinte mensagem aparece:

   `A transmissão do evento de serviço de teste foi iniciada`

   `Transmissão do evento de serviço em andamento.`

   Quando a transmissão estiver concluída, o evento de teste será listado no Log de eventos de serviço e no Insight RS Console. Se o teste tiver êxito, a coluna Status do envio mostrará o texto *Sem erros*.

A coluna Hora de criação, no Log de eventos de serviço, mostra a data e a hora com base no fuso horário do iLO configurado.

5. Confira o Insight RS Console para verificar se o evento de teste chegou:
   a. Faça logon no Insight RS Console.
   b. No Menu principal, selecione **Dispositivos**.
   c. Localize o servidor ProLiant e clique no nome do dispositivo.
   d. Clique na guia **Eventos de serviços**. Todos os eventos de serviço enviados em relação ao sistema são mostrados na tela Eventos de serviço (mesmo se você limpar o log de eventos de serviço).

      O Insight RS converte o valor de hora de geração do evento de serviço do iLO no fuso horário do navegador usado para acessar o Insight RS Console.

      **Observação:** Os eventos de teste são automaticamente fechados pela HP, já que nenhuma ação mais é necessária.

# Iniciar uma coleta de dados

Você pode testar as coletas usando a interface Web do iLO 4 ou o Insight RS Console. Coletas não são executadas automaticamente depois da descoberta. A HP recomenda que você execute uma coleta manualmente após a descoberta completa para verificar a conectividade.

**Observação:** O Insight Remote Support executará uma coleta de dados quando o servidor ProLiant for descoberto. Se você gerar uma coleta de dados manualmente usando um dos métodos descritos abaixo, aparecerão duas coletas de dados para o dispositivo no Insight RS Console.

## *Iniciar uma coleta de dados na interface da Web do iLO 4*

Para iniciar uma coleta de dados na interface da Web do iLO 4, conclua as seguintes etapas:

1. Faça logon na interface da Web do iLO4 (`https://`*`<nome de host ou endereço IP do iLO>`*).
2. Navegue até **Remote Support** → **Coletas de dados**. Aparece a tela Coletas de dados.
3. Clique em **Enviar coleta de dados**.
4. Clique em **OK** para confirmar a ação. Quando a transmissão terminar, a data e a hora da transmissão de coleta de dados mais recente será atualizada.

O iLO envia a coleta de dados para o Insight RS. No Insight RS Console, você pode exibir os resultados na tela Serviços de coleta → Resultados da coleta básica.

## *Iniciar uma coleta de dados no Insight Remote Support*

Para iniciar uma coleta de dados no Insight Remote Support, conclua as seguintes etapas:

1. Faça logon no Insight RS Console.
2. Navegue até **Serviços de coleta** → **Agendamentos de coleta**.
3. No painel Lista de agendamentos de coleta, selecione **Agendamento de coleta básica na configuração do servidor**.
4. No painel Informações de agendamento, clique em **Executar agora**.

O Insight Remote Support executa o agendamento. Você pode exibir os resultados na guia Resultados da coleta básica.

# Enviar um relatório do AHS (sistema de integridade ativo)

**Observação:** O Insight Remote Support executa uma relatório do AHS (sistema de integridade ativo) quando o servidor ProLiant é detectado. Se você enviar um relatório do AHS (sistema de integridade ativo) usando um dos métodos descritos abaixo, dois relatórios do AHS aparecerão para o dispositivo no Insight RS Console.

## *Enviar um relatório do AHS (sistema de integridade ativo) na interface da Web do iLO 4*

Para enviar um relatório do AHS (sistema de integridade ativo) na interface da Web do iLO 4, conclua as seguintes etapas:

1. Faça logon na interface da Web do iLO (`https://`*`<nome de host ou endereço IP do iLO>`*).
2. Navegue até **Remote Support** → **Coletas de dados**. Aparece a tela Coletas de dados.
3. Clique em **Enviar relatório do AHS (sistema de integridade ativo)**.

4. Clique em **OK** para confirmar a ação. Quando a transmissão terminar, a data e a hora da transmissão mais recente do relatório do AHS (sistema de integridade ativo) serão atualizadas.

O iLO envia o relatório do AHS (sistema de integridade ativo) ao Insight RS. No Insight RS Console, você pode exibir os resultados na tela Serviços de coleta → Resultados da coleta básica.

### *Enviar um relatório do AHS (sistema de integridade ativo) no Insight Remote Support*

Para enviar um relatório do AHS (sistema de integridade ativo) no Insight RS Console, conclua as seguintes etapas:

1. Faça logon no Insight RS Console.
2. Navegue até **Serviços de coleta** → **Agendamentos de coleta**.
3. No painel Lista de agendamentos de coleta, clique em **Coleta AHS**.
4. No painel Informações de agendamento, clique em **Executar agora**.

O Insight Remote Support executa o agendamento. Você pode exibir os resultados na guia Resultados da coleta básica.

Para conhecer tarefas de manutenção e solução de problemas, expanda a seguinte seção:

# Manutenção e solução de problemas

As seguintes tarefas de manutenção estão disponíveis para servidores ProLiant Gen8 e Gen9:

## Definir o modo de manutenção

Certifique-se de ativar o Modo de manutenção quando for fazer trabalho de manutenção no servidor ProLiant. Quando no modo de manutenção, os eventos ou mensagens enviados para o Insight Remote Support são sinalizados para indicar que nenhuma providência precisa ser tomada para o evento.

Para definir o modo de manutenção, conclua as seguintes etapas:

1. No menu de navegação, clique em **Remote Support** → **Eventos de serviço**. Aparece a tela Eventos de serviço.
2. Na seção Modo de manutenção do servidor, marque a caixa de seleção **Definir modo de manutenção**. Aparece a lista suspensa **Expira em**.

3. Na lista suspensa **Expira em**, selecione por quanto tempo você trabalhará no servidor ProLiant.
4. Clique em **Aplicar**.

**Observação:** O modo de manutenção termina depois que tiver passado o tempo especificado. Você pode encerrar o modo de manutenção antes, selecionando a opção **Sair do modo de manutenção** e clicando em **Aplicar**. Aparece uma mensagem de confirmação.

# Desativar o monitoramento de um servidor ProLiant Gen8 e Gen9

Por algum motivo, talvez você precise desconectar um servidor ProLiant para que ele não seja mais reconhecido pelo Insight Remote Support. Por exemplo, se a garantia do servidor tiver expirado ou se você tiver mudado recentemente o dispositivo host.

Se quiser desabilitar temporariamente o monitoramento do seu servidor HP ProLiant, desabilite o dispositivo no Insight RS Console. Se quiser desabilitar temporariamente o monitoramento do seu servidor HP ProLiant, exclua o dispositivo no Insight RS Console.

Para desabilitar temporariamente o monitoramento, siga estas instruções:

**Observação:** Cancelar o registro diretamente na interface Web do iLO 4 é o mesmo que desabilitar temporariamente o dispositivo no Insight RS Console.

1. No Insight RS Console, navegue até **Dispositivos** → **Resumo de dispositivos**.
2. Na coluna mais à esquerda, marque a caixa de seleção dos dispositivos que você deseja desabilitar.
3. Clique em **Ações** → **Desabilitar selecionados** e em **OK** na caixa de diálogo de confirmação.

Para desabilitar permanentemente o monitoramento, siga estas instruções:

1. No Insight RS Console, navegue até **Dispositivos** → **Resumo de dispositivos**.
2. Na coluna mais à esquerda, marque a caixa de seleção dos dispositivos que serão excluídos.
3. Clique em **Ações** → **Excluir selecionados** e depois em **OK** na caixa de diálogo de confirmação.

Os seguintes problemas conhecidos aplicam-se a servidores ProLiant Gen8 e Gen9:

# Endereço IP faltando durante a detecção

Após a detecção de um servidor ProLiant por meio da interface da Web do iLO 4, o servidor pode se identificar pelo número de série (indicado por um prefixo S/N) na coluna Nome do dispositivo do Insight RS Console.

Para mostrar o servidor ProLiant por nome de host ou endereço IP, siga estas instruções:

1. Verifique se os seguintes pré-requisitos são atendidos:
   - **Firmware do iLO**
     - Para servidores HP ProLiant Gen8: A versão 1.10 ou posterior é necessária.
     - Para servidores HP ProLiant Gen9: A versão 2.00 ou posterior é necessária.

   **Importante:** Para solucionar vulnerabilidades de softwares de terceiros, a HP recomenda o uso do iLO 4 2.03 ou versão posterior. Para acessar a interface Web do iLO 4 2.03 ou versão posterior, você deve habilitar o TLS no seu navegador. O TLS é o sucessor do SSL (Secure Sockets Layer).

   - **AMS**—O serviço de gerenciamento sem agente (AMS) está habilitado e o sistema operacional está sendo executado.
   - **RIBCL** — As credenciais do protocolo RIBCL do iLO para o servidor são configuradas no Insight RS Console e atribuídas ao servidor ProLiant.
2. Faça logon no Insight RS Console.
3. Navegue até **Dispositivos** → **Resumo do dispositivo**.
4. Clique no número de série, na coluna Nome do dispositivo.
5. Na guia **Dispositivo**, expanda a seção **Status** e clique em **Detectar dispositivo**. Quando o dispositivo for detectado novamente, o nome de host ou o endereço IP será mostrado.

   **Observação:** A configuração DNS determina se o nome de host ou endereço IP é mostrado.

# Discrepância da garantia e contrato no Insight Online

Pode ocorrer uma discrepância no Insight Online entre o Status de suporte na seção Garantias vinculadas e o Status de suporte na parte superior da tela. O número de série do ProLiant usado tem uma garantia válida, e a seção Garantia vinculada confirma que a garantia está *Ativa*. Porém, o Status de suporte no alto da tela está listado como *Expirado*.

A discrepância ocorre quando o endereço do site configurado no Insight Remote Support não é um endereço válido. Sem um endereço válido, o Insight Online não consegue determinar o código do país e, por isso, ele tenta obter o código a partir do perfil do HP Passaporte (HPP) usado para autorização. Como o código do país não é necessário no HPP, talvez ele não tenha sido fornecido. Nesse caso, quando o código do país está faltando durante a verificação do direito, aparece o status `Expirado`.

Para resolver esse problema, verifique se o endereço do cliente na guia Insight RS Console em **Company Information** → **Sites** é válido, sem abreviações para nomes de ruas ou cidades, e certifique-se de que as informações do site estão aplicadas ao dispositivo no qual está ocorrendo a discrepância.

# Capítulo 3: Configurar servidores ProLiant Windows

O Insight Remote Support (RS) deve ser capaz de se comunicar com o servidor ProLiant para que ele possa ser monitorado. O Insight RS pode se comunicar com servidores ProLiant executando o Windows com o WMI ou o SNMP. As informações a seguir descrevem como instalar e configurar os protocolos de comunicação e outros componentes de software recomendados para que eles possam ser monitorados pelo Insight RS.

Use essas instruções de configuração para o Windows 2003, Windows 2008 e Windows 2012.

Se tanto o SNMP quanto o WMI estiverem disponíveis no dispositivo ProLiant Windows monitorado, recomenda-se que um dos protocolos seja desativado no Insight RS Console para evitar notificações duplicadas sobre falhas em um componente único. Desative o SNMP se não houver dispositivos de armazenamento smart separados, como MSAs ligados ao dispositivo monitorado. Se houver dispositivos de armazenamento smart separados, desative o protocolo WMI no Insight RS Console. Para tal, exclua o protocolo do dispositivo monitorado no Insight RS Console.

**Importante:** Para reunir coletas SAN para um servidor ProLiant Windows, você deve usar o WMI e o Service Pack para o ProLiant versão 2.8 ou posterior.

Para configurar seu servidor ProLiant Windows usando o WMI, consulte "Configurar servidores ProLiant Windows usando o WMI".

Para configurar seu servidor ProLiant Windows usando o SNMP, consulte "Configurar servidores ProLiant Windows usando o SNMP".

## Configurar servidores ProLiant Windows usando o WMI

O Insight Remote Support (RS) deve ser capaz de se comunicar com o servidor ProLiant para que ele possa ser monitorado. O Insight RS pode se comunicar com servidores ProLiant executando o Windows com WMI. As informações a seguir descrevem como instalar e configurar o WMI e outros componentes de software recomendados, para que eles possam ser monitorados pelo Insight RS.

Essas instruções de configuração podem ser usadas para Windows 2003, Windows 2008 e Windows 2012.

### Atender aos requisitos de configuração

Para configurar servidores ProLiant Windows usando o WMI de forma que eles sejam monitorados pelo Insight RS, conclua as seguintes seções:

**Tabela 3.1** ***Etapas de configuração do servidor ProLiant Windows usando o WMI***

| Tarefa | Concluída? |
|---|---|
| Verifique o *Notas de Lançamento do HP Insight Remote Support*, para garantir que o seu servidor ProLiant Windows seja suportado. | |

**Tabela 3.1** ***Etapas de configuração do servidor ProLiant Windows usando o WMI, continuação***

| Tarefa | Concluída? |
| --- | --- |
| Instale o WBEM/WMI no servidor ProLiant Windows, disponível no Service Pack para ProLiant (SPP). | |
| Adicione o protocolo WMI ao Insight RS Console. | |
| Detecte o servidor ProLiant Windows no Insight RS Console. | |
| Envie um evento de teste para verificar a conectividade entre o seu servidor ProLiant Windows e o Insight RS. | |

# Instalar e configurar o software de comunicação em servidores

Para configurar seus dispositivos monitorados, conclua as seguintes seções:

# Instalar e configurar o WMI

## Instalar o Service Pack para ProLiant

O Service Pack para ProLiant (SPP) é um pacote de software que inclui drivers, utilitários e agentes de gerenciamento para o(s) dispositivo(s) ProLiant. O SPP vem incluído no HP SmartStart CD fornecido com o ProLiant. A versão mais atual também está disponível em: http://www.hp.com/go/spp/download.

Sistemas HP ProLiant com Microsoft Windows são suportados pelo Insight Management Providers (IM Providers para suporte a WBEM/WMI Mapper). Os provedores e agentes estão disponíveis na mesma mídia do SPP.

**Importante:** Para reunir coletas SAN para um servidor ProLiant Windows, você deve usar o WMI e o Service Pack para o ProLiant versão 2.8 ou posterior.

Se o SNMP estiver disponível no dispositivo ProLiant Windows monitorado, recomenda-se que o WBEM seja desativado no Insight RS Console para evitar notificações duplicadas sobre falhas em um componente único. Para tal, exclua o protocolo SNMP do dispositivo monitorado no Insight RS Console.

## Instalar o WMI

Os IM Providers do SmartStart CD e/ou do SPP versão 8.1 e posterior são compatíveis com o Insight Remote Support.

Consulte o site da web dos *Provedores de WBEM do HP Insight Management*, em: http://h18013.www1.hp.com/products/servers/management/wbem/, para mais informações sobre provedores WBEM, segurança e credenciais.

Se estiver usando o Windows WBEM Providers (IM Providers), as credenciais do WBEM deverão ser definidas para cada dispositivo monitorado no Insight RS Console para que ele possa ser monitorado. Se você alterar suas credenciais do WBEM a qualquer momento, *deverá* modificar a entrada dessas credenciais no Insight RS Console.

Os Provedores WBEM IM são opcionais na instalação do SPP. Certifique-se de selecioná-los durante a instalação do SPP.

## Instalar a System Management Homepage

O System Management Homepage (SMH) também faz parte do SPP. Ele fornece recursos adicionais de relatório sobre o dispositivo monitorado. Mesmo que não seja obrigatório para o Insight Remote Support, o SMH pode ser usado para operar com o protocolo WBEM, por exemplo, para enviar eventos de teste.

## Desativar o controle de conta de usuário no Windows 2008

No Windows 2008, o WMI não consegue se conectar ao namespace root\WMI se o User Account Control (Controle de Conta de Usuário, UAC) estiver ativado. Use um dos procedimentos abaixo para desativar o UAC, conforme a versão do Windows 2008 que você estiver usando. Para realizar esse procedimento, você precisa se conectar como administrador local ou fornecer as credenciais de um membro do grupo de administradores locais.

Para desativar o UAC no Windows 2008, conclua as seguintes etapas:

1. Clique em **Iniciar** e em **Painel de controle**.
2. No painel de controle, clique em **Contas de usuário**.
3. Na janela Contas de usuário, clique em **Contas de usuário**.
4. Na janela de tarefas User Accounts (Contas de usuário), clique em **Ativar ou desativar o Controle de Conta de Usuário**.
5. Se o UAC estiver configurado no Modo de Aprovação de Administrador, aparecerá a mensagem Controle de Conta de Usuário. Clique em **Continuar**.
6. Desmarque a caixa de seleção **Utilizar o Controle de Conta de Usuário (UAC) para ajudar a proteger o computador**, depois clique em **OK**.
7. Clique em **Reiniciar agora** para aplicar as modificações imediatamente, ou clique em **Reiniciar mais tarde**, depois feche a janela de tarefa Contas de usuário.

Para desativar o UAC no Windows 2008 R2 e no Windows 2012, conclua as seguintes etapas:

1. Clique em **Iniciar** e em **Painel de controle**.
2. No painel de controle, clique em **Contas de usuário**.
3. Na janela Contas de usuário, clique em **Contas de usuário**.
4. Na janela de tarefas Contas de usuário, clique em **Alterar configurações de Controle de Conta de Usuário**.
5. Se aparecer a caixa de diálogo Controle de conta de usuário, certifique-se de que a ação exibida é o que você deseja, depois clique em **Sim**.
6. Na página Configurações do controle de conta de usuário, desative o UAC: mova a barra deslizante para **Nunca notificar** e clique em **OK**.
7. Reinicie o servidor para aplicar as alterações.

## *Definir configurações de firewall e porta*

Para obter uma lista completa de requisitos de firewall e de porta para dispositivos monitorados, consulte o *Informe de Segurança do HP Insight Remote Support*, em: http://www.hp.com/go/insightremotesupport/docs.

# Adicionar credenciais de protocolo e iniciar a detecção

Para detectar seus dispositivos monitorados, conclua as seguintes seções:

## *Criar uma credencial de protocolo WMI no Insight RS Console*

Para configurar o WMI no Insight RS Console, conclua as seguintes etapas:

1. Em um navegador da Web, faça logon no Insight RS Console.
2. No menu principal, selecione **Detecção** e clique na guia **Credenciais**.
3. Na lista suspensa **Selecionar e configurar protocolo**, selecione **Instrumentação de Gerenciamento do Windows (WMI)**.

4. Clique em **Novo**. A caixa de diálogo Nova credencial é exibida.
5. Digite o nome de usuário e a senha configurados no seu dispositivo.
6. Clique em **Adicionar**.

O Insight RS cria a credencial de protocolo, que é exibida na tabela de credenciais.

### Detectar o dispositivo no Insight RS Console

Para detectar o dispositivo por meio do Insight RS Console, conclua as seguintes etapas:

1. Em um navegador da Web, faça logon no Insight RS Console.
2. No menu principal, selecione **Detecção** e clique na guia **Fontes**.
3. Expanda a seção Endereços IP e adicione o endereço IP do seu dispositivo:
   a. Clique em **Novo**.
   b. Selecione **Endereço único**, **Intervalo de endereços** ou **Lista de endereços**.
   c. Digite os endereços IP dos dispositivos a serem detectados.
   d. Clique em **Adicionar**.
4. Clique em **Iniciar detecção**.

### Verificar o status de detecção e do dispositivo

Para verificar se o dispositivo foi detectado corretamente, conclua as seguintes etapas:

1. Em um navegador da Web, faça logon no Insight RS Console.
2. No menu principal, selecione **Dispositivos** e clique na guia **Resumo do dispositivo**.
3. Verifique se a coluna Status contém um ícone de êxito ( ).

   Se não houver ícone de êxito, tente descobrir que coluna está com problema e consulte a Ajuda on-line para informações de solução de problemas.

## Verificar a comunicação entre o dispositivo monitorado e o Insight RS

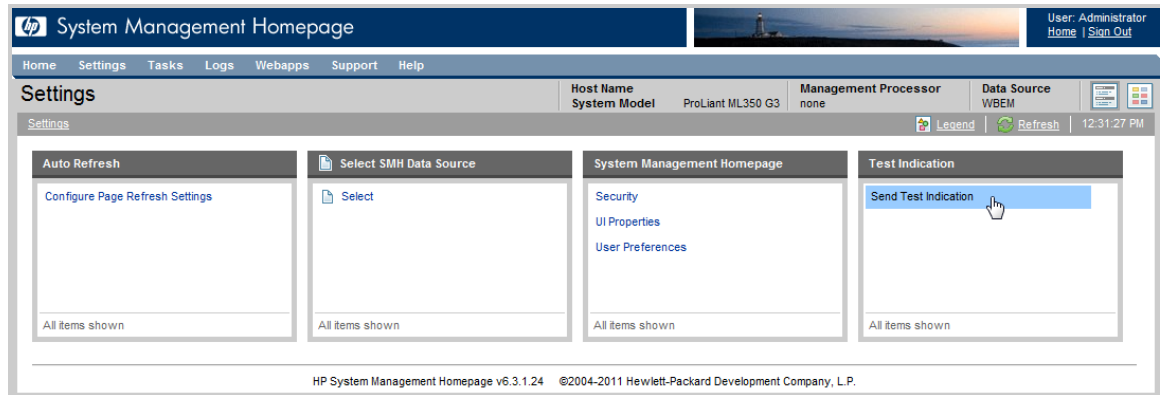
Para verificar a comunicação entre o dispositivo monitorado e o Insight RS, conclua as seguintes seções:

### Enviar uma indicação de teste do WBEM ao dispositivo host

Para verificar a conectividade do dispositivo monitorado com o dispositivo host, envie uma indicação de teste do WBEM ao dispositivo host e verifique se a indicação de teste foi recebida no Insight RS Console.

1. Em um navegador, acesse o System Management Homepage (SMH) no dispositivo monitorado: `https://[endereçoIP]:2381`.
2. Faça login usando o nome do usuário administrador e a senha do dispositivo monitorado.

se não aparecer a tela de login, clique no link **Entrar** no canto superior direito da interface da SMH. Se você não estiver conectado como administrador do dispositivo monitorado, não terá todas as opções de configuração relevantes.

3. Na barra superior do menu, clique em **Configurações**.

4. Se você tiver optado pela instalação de WBEM com o SPP, ele será definido como sua fonte de dados. No painel Indicação de teste, clique em **Enviar indicação de teste**.

5. Na tela **Enviar indicação de teste**, selecione um tipo de ID de evento (pode ser qualquer uma) e clique em **Enviar**.

## Visualizar eventos de teste no Insight RS Console

Alguns tipos de dispositivos monitorados permitem o envio de um evento de teste ao Insight Remote Support. Depois de configurar o dispositivo monitorado e enviar um evento de teste, use o seguinte processo para verificar se o evento de teste chegou.

1. Faça logon no Insight RS Console.
2. No menu principal, selecione **Eventos de serviços**. Se o dispositivo monitorado estiver configurado

adequadamente, o evento aparecerá no painel Informações sobre eventos de serviços.

## Verificar coletas no Insight RS Console

Coletas não são executadas automaticamente depois da descoberta. A HP recomenda que você execute uma coleta manualmente após a descoberta completa para verificar a conectividade. Execute o cronograma de coleta manualmente na guia Serviços de coleta → Agendamentos de coleta. Para obter mais informações sobre o agendamento de coletas, consulte a Ajuda do Insight RS.

Verifique se essa coleta foi bem-sucedida na guia Serviços de coleta → Resultados da coleta básica do Insight RS Console.

1. Faça logon no Insight RS Console.
2. No menu principal, selecione **Serviços de coleta** e depois clique na guia **Resultados da coleta básica**.
3. Expanda a seção Coleta de configurações básicas do servidor.
4. Localize a entrada referente ao seu dispositivo e verifique a coluna Resultado. Se a coleta tiver sido bem-sucedida, um ícone de êxito será exibido (). Se ocorrer uma falha, um ícone de erro será exibido ().

# Manutenção e solução de problemas

As seguintes tarefas de solução de problemas estão disponíveis para servidores ProLiant Windows que usam o WMI:

## Integridade de dispositivos no Insight Remote Support

Se você estiver usando o SNMP para dar suporte ao Windows Server, e o servidor tiver o serviço WMI ativado, a integridade do dispositivo no Insight RS Console poderá exibir um ícone de erro () se credenciais inválidas do WMI tiverem sido associadas ao servidor no Insight RS Console.

Se isso ocorrer, a integridade do servidor exibirá um ícone de erro, porque o Insight RS não consegue configurar o WMI. Para resolver o problema, siga uma destas etapas:

- Remova as credenciais WMI padrão e só as associe aos dispositivos que com certeza têm provedores WMI instalados.

  ou

- Corrija as credenciais do WMI conectado ao servidor no Insight RS Console.

# Configurar servidores ProLiant Windows usando o SNMP

O Insight Remote Support (RS) deve ser capaz de se comunicar com o servidor ProLiant para que ele possa ser monitorado. O Insight RS pode se comunicar com servidores ProLiant executando o Windows com SNMP. As informações a seguir descrevem como instalar e configurar os protocolos de comunicação e outros componentes de software recomendados para que eles possam ser monitorados pelo Insight RS.

Use essas instruções de configuração para o Windows 2003, Windows 2008 e Windows 2012.

# Atender aos requisitos de configuração

Para configurar servidores ProLiant Windows usando o SNMP de forma que eles sejam monitorados pelo Insight RS, conclua as seguintes seções:

**Tabela 3.2** ***Etapas de configuração do servidor ProLiant Windows usando o SNMP***

| Tarefa | Concluída? |
|---|---|
| Verifique o *Notas de Lançamento do HP Insight Remote Support*, para garantir que o seu servidor ProLiant Windows seja suportado. | |
| Instale o SNMP no servidor ProLiant Windows, disponível no Service Pack para ProLiant (SPP). | |
| Configure o SNMP no servidor ProLiant Windows. | |
| Adicione o protocolo SNMP ao Insight RS Console. | |
| Detecte o servidor ProLiant Windows no Insight RS Console. | |
| Envie um evento de teste para verificar a conectividade entre o seu servidor ProLiant Windows e o Insight RS. | |

# Instalar e configurar o software de comunicação em servidores

Para configurar seus dispositivos monitorados, conclua as seguintes seções:

## *Instalar e configurar agentes SNMP*

### *Instalar o Service Pack para ProLiant*

O Service Pack para ProLiant (SPP) é um pacote de software que inclui drivers, utilitários e agentes de gerenciamento para o(s) dispositivo(s) ProLiant. O SPP vem incluído no HP SmartStart CD fornecido

com o ProLiant. A versão atual também está disponível em: http://www.hp.com/go/spp/download.

Sistemas HP ProLiant com Microsoft Windows são suportados pelo Insight Management Agents (IM Agents para suporte SNMP). Os provedores e agentes estão disponíveis na mesma mídia do SPP.

Se o WBEM estiver disponível no dispositivo ProLiant Windows monitorado, recomenda-se que o WBEM seja desativado no Insight RS Console para evitar notificações duplicadas sobre falhas em um componente único. Para tal, exclua o protocolo WMI do dispositivo monitorado no Insight RS Console.

Se estiver usando Agentes SNMP do Windows (Agentes IM), você deverá configurar o SNMP para se comunicar com o dispositivo host (consulte "Configurar o SNMP").

### *Instalar a System Management Homepage*

O System Management Homepage (SMH) também faz parte do SPP. Ele fornece recursos adicionais de relatório sobre o dispositivo monitorado. Embora não seja obrigatório para o Insight Remote Support, se você não tiver configurado serviços SNMP corretamente para comunicação com o dispositivo host durante a instalação do Insight Management Agent, poderá usar o SMH para refazer essas configurações. Se você tiver instalado a configuração padrão de SNMP e a configuração WMI opcional durante a instalação do SPP, o padrão da SMH será a configuração WMI, e pode ser que você precise restaurá-la para a configuração SNMP se optar por receber eventos de hardware através do SNMP.

### *Configurar o SNMP*

Os dispositivos monitorados devem ser configurados para se comunicar com o dispositivo host. Se você optar por usar o SNMP, as seguintes etapas serão necessárias para permitir que os dispositivos monitorados se comuniquem totalmente com o dispositivo host.

Dispositivos monitorados que usam notificações SNMP devem incluir o seguinte:

- Todos os dispositivos monitorados devem ter uma conexão de intranet em funcionamento, como através de um adaptador Ethernet, com o TCP/IP instalado e funcionando. Os dispositivos monitorados devem ter comunicação bidirecional com o dispositivo host através dessa conexão.
- Todos os dispositivos monitorados precisam do software Insight Management Agent para detecção de problemas e geração de armadilhas. Os agentes IM são distribuídos pela HP e projetados para gerar interceptações SNMP com informações que possibilitam uma análise mais completa.
- Todos os dispositivos monitorados precisam ter o endereço de IP do dispositivo host definido como um destino de armadilha.

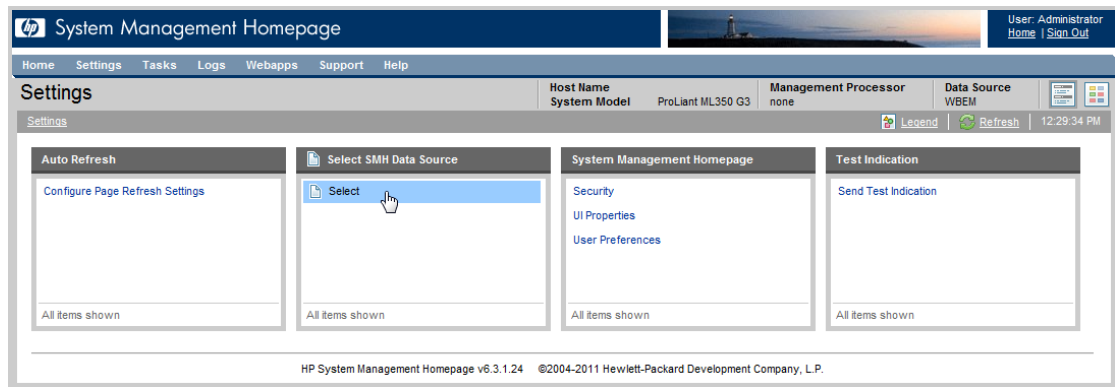
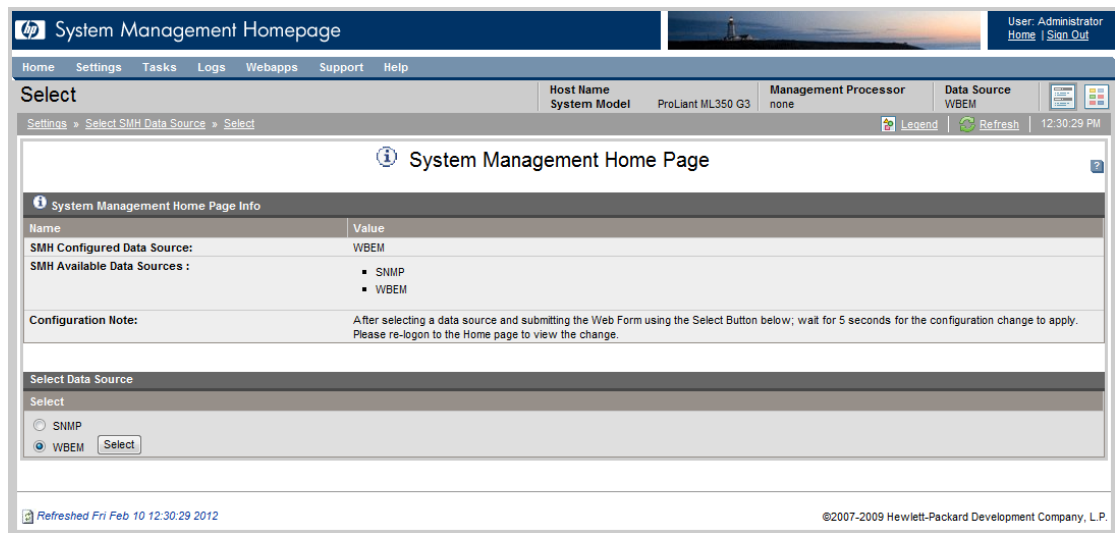
O dispositivo host precisa ser capaz de se comunicar com o dispositivo monitorado mas, por padrão, o Windows Server só aceita pacotes SNMP do host local. Para configurar o servidor Windows para enviar interceptações para o dispositivo host, siga estas etapas:

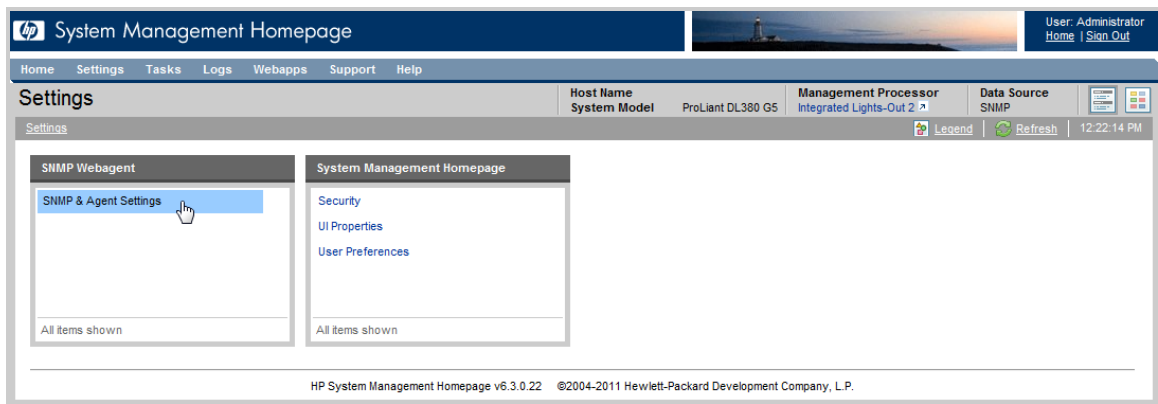
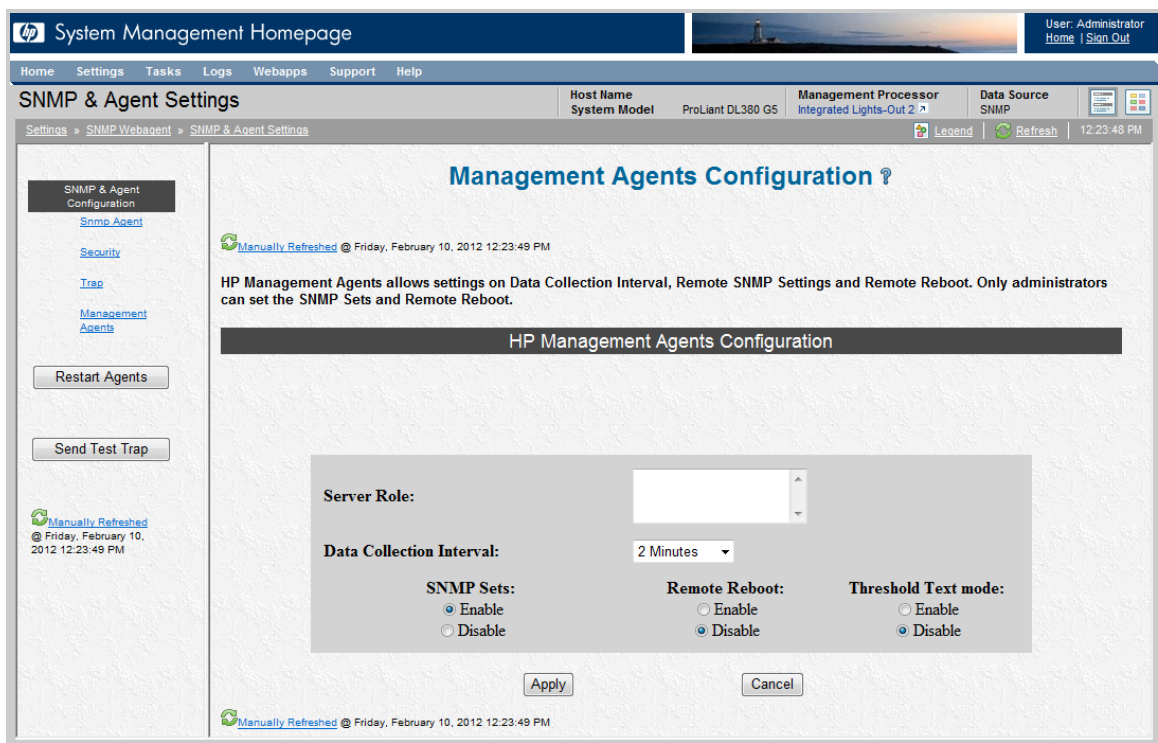
1. Em um navegador, acesse o System Management Homepage (SMH) no dispositivo monitorado: `https://[`*`endereçoIP`*`]:2381`.
2. Faça login usando o nome do usuário administrador e a senha do dispositivo monitorado.

   se não aparecer a tela de login, clique no link **Entrar** no canto superior direito da interface da SMH. Se você não tiver feito login como administrador, não terá todas as opções de configuração relevantes.
3. Na barra superior do menu, clique em **Configurações**.

Se **Configurações** exibir a imagem abaixo, significa que o WBEM está configurado como a fonte de dados. Primeiro, será preciso configurar sua fonte de dados como SNMP. Se o SNMP já estiver definido como sua fonte de dados, pule para a próxima etapa.

Para alterar a fonte de dados para SNMP, siga estas instruções:

a. No painel **Selecionar fonte de dados na SMH**, clique no link **Selecionar**.

b. No painel Selecionar fonte de dados, selecione a opção SNMP e clique em **Selecionar**.

c. Na barra superior do menu, clique em **Configurações**. Se você tiver alterado a fonte de dados para SNMP enquanto estava conectado remotamente com a SMH, terá que fazer login de novo e clicar na guia **Configurações**.

4. No painel **SNMP Webagent**, clique no link **Configuração de SNMP e agente**.

5. No menu esquerdo da tela Configuração do Management Agents, clique no link **Segurança**.

6. Na tela Configuração de segurança, selecione uma destas opções na seção Hosts selecionados:

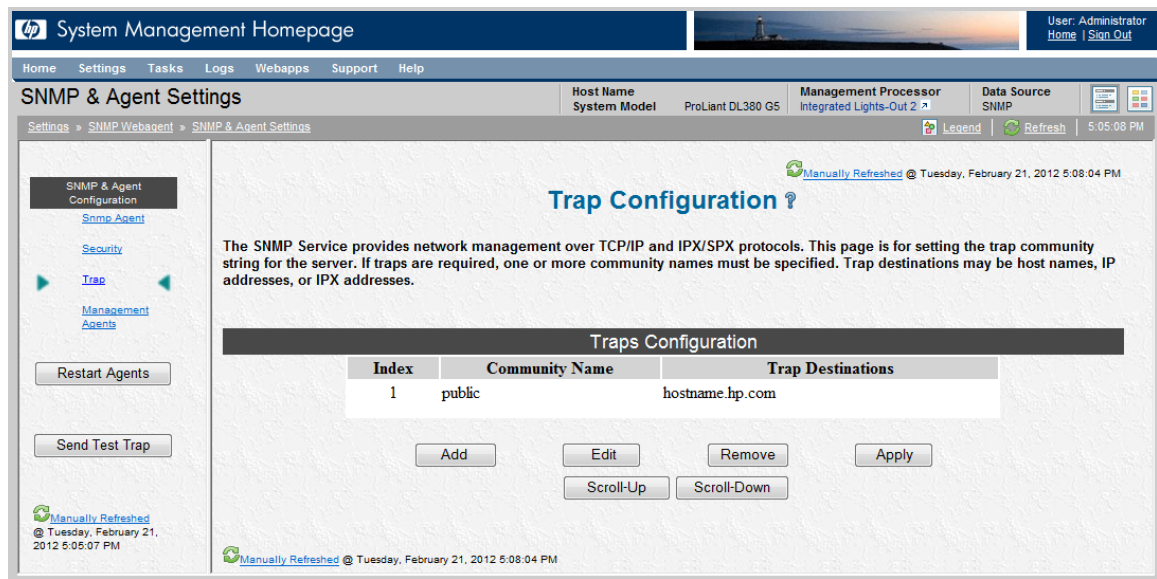
- **Aceitar pacotes SNMP de qualquer host.**

  ou

- **Aceitar pacotes SNMP destes hosts** e especificar o endereço de IP de seu dispositivo host na área de texto.

7. No menu esquerdo da tela Configuração de segurança, clique no link **Armadilha**.
8. Na tela Configuração de armadilha, siga um destes procedimentos:
   - Adicione um Nome de comunidade que inclua o dispositivo host como destino de interceptação.

     ou

   - Edite o Nome de comunidade público de modo a incluir o Dispositivo host como Destino de armadilha.

Siga as instruções anteriores para cada dispositivo ProLiant Windows monitorado que use SNMP para se comunicar com o dispositivo host.

## Definir configurações de firewall e porta

Para obter uma lista completa de requisitos de firewall e de porta para dispositivos monitorados, consulte o *Informe de Segurança do HP Insight Remote Support*, em: http://www.hp.com/go/insightremotesupport/docs.

# Adicionar credenciais de protocolo e iniciar a detecção

Para detectar seus dispositivos monitorados, conclua as seguintes seções:

## Criar uma credencial de protocolo SNMP no Insight RS Console

Se a cadeia da comunidade SNMP do dispositivo estiver definida como `pública` e o modo de acesso da comunidade for `somente leitura`, o Insight RS associará automaticamente um protocolo SNMP ao seu dispositivo. Se você usar uma cadeia de comunidade diferente ou uma porta não padrão, precisará criar uma credencial de protocolo SNMP no Insight RS Console.

Para configurar o SNMP no Insight RS Console, conclua as seguintes etapas:

1. Em um navegador da Web, faça logon no Insight RS Console.
2. No menu principal, selecione **Detecção** e clique na guia **Credenciais**.
3. Na lista suspensa Selecionar e configurar protocolo:, selecione **Simple Network Management Protocol** para a versão do SNMP configurada no servidor.
4. Clique em **Novo**. A caixa de diálogo Nova credencial é exibida.
5. Digite as informações configuradas no seu servidor.
6. Clique em **Adicionar**.

O Insight RS cria a credencial de protocolo, que é exibida na tabela de credenciais.

### Detectar o dispositivo no Insight RS Console

Para detectar o dispositivo por meio do Insight RS Console, conclua as seguintes etapas:

1. Em um navegador da Web, faça logon no Insight RS Console.
2. No menu principal, selecione **Detecção** e clique na guia **Fontes**.
3. Expanda a seção Endereços IP e adicione o endereço IP do seu dispositivo:
   a. Clique em **Novo**.
   b. Selecione **Endereço único**, **Intervalo de endereços** ou **Lista de endereços**.
   c. Digite os endereços IP dos dispositivos a serem detectados.
   d. Clique em **Adicionar**.
4. Clique em **Iniciar detecção**.

### Verificar o status de detecção e do dispositivo

Para verificar se o dispositivo foi detectado corretamente, conclua as seguintes etapas:

1. Em um navegador da Web, faça logon no Insight RS Console.
2. No menu principal, selecione **Dispositivos** e clique na guia **Resumo do dispositivo**.
3. Verifique se a coluna Status contém um ícone de êxito ().

   Se não houver ícone de êxito, tente descobrir que coluna está com problema e consulte a Ajuda on-line para informações de solução de problemas.

## Verificar a comunicação entre o dispositivo monitorado e o Insight RS

Para verificar a comunicação entre o dispositivo monitorado e o Insight RS, conclua as seguintes seções:

### Enviar uma interceptação de teste SNMP para o dispositivo host

Para verificar a conectividade do dispositivo monitorado com o dispositivo host, envie uma interceptação de teste SNMP ao dispositivo host e verifique se essa interceptação de teste foi recebida no Insight RS Console.

1. Em um navegador, acesse o System Management Homepage (SMH) no dispositivo monitorado: `https://[endereçoIP]:2381`.
2. Faça login usando o nome do usuário administrador e a senha do dispositivo monitorado.

   se não aparecer a tela de login, clique no link **Entrar** no canto superior direito da interface da SMH. Se você não tiver feito login como administrador, não terá todas as opções de configuração relevantes.
3. Na barra superior do menu, clique em **Configurações**.

   Se você tiver instalado o WBEM com o SPP, ele pode estar definido como sua fonte de dados. Se for esse o caso, consulte "Configurar o SNMP" para obter informações sobre como configurar a fonte de dados como SNMP.

4. No painel SNMP Webagent, clique no link **Configuração de SNMP e agente**.
5. No menu esquerdo, clique em **Enviar armadilha de teste**.

## Visualizar eventos de teste no Insight RS Console

Alguns tipos de dispositivos monitorados permitem o envio de um evento de teste ao Insight Remote Support. Depois de configurar o dispositivo monitorado e enviar um evento de teste, use o seguinte processo para verificar se o evento de teste chegou.

1. Faça logon no Insight RS Console.
2. No menu principal, selecione **Eventos de serviços**. Se o dispositivo monitorado estiver configurado adequadamente, o evento aparecerá no painel Informações sobre eventos de serviços.

## Verificar coletas no Insight RS Console

Coletas não são executadas automaticamente depois da descoberta. A HP recomenda que você execute uma coleta manualmente após a descoberta completa para verificar a conectividade. Execute o cronograma de coleta manualmente na guia Serviços de coleta → Agendamentos de coleta. Para obter mais informações sobre o agendamento de coletas, consulte a Ajuda do Insight RS.

Verifique se essa coleta foi bem-sucedida na guia Serviços de coleta → Resultados da coleta básica do Insight RS Console.

1. Faça logon no Insight RS Console.
2. No menu principal, selecione **Serviços de coleta** e depois clique na guia **Resultados da coleta básica**.
3. Expanda a seção Coleta de configurações básicas do servidor.
4. Localize a entrada referente ao seu dispositivo e verifique a coluna Resultado. Se a coleta tiver sido bem-sucedida, um ícone de êxito será exibido (). Se ocorrer uma falha, um ícone de erro será exibido ().

# Capítulo 4: Configurar servidores ProLiant Linux

## Atender aos requisitos de configuração

Para configurar servidores ProLiant Linux de forma que eles sejam monitorados pelo Insight RS, conclua as seguintes seções:

**Tabela 4.1** ***Etapas de configuração do servidor ProLiant Linux***

| Tarefa | Concluída? |
|---|---|
| Certifique-se de que o Insight RS suporte seu servidor ProLiant Linux, verificando o *Notas de Lançamento do HP Insight Remote Support*. | |
| Instale o SNMP no servidor ProLiant Linux, disponível no Service Pack para ProLiant (SPP). | |
| Configure o SNMP no servidor ProLiant Linux. | |
| Adicione o protocolo SNMP ao Insight RS Console. | |
| Detecte o servidor ProLiant Linux no Insight RS Console. | |
| Envie um evento de teste para verificar a conectividade entre seu servidor ProLiant Linux e o Insight RS. | |

## Instalar e configurar o software de comunicação em servidores

Para configurar seus dispositivos monitorados, conclua as seguintes seções:

### Instalar agentes SNMP

O Service Pack para ProLiant (SPP) é um pacote de software específico de sistema que inclui drivers, utilitários e agentes de gerenciamento para seu(s) dispositivo(s) ProLiant. O SPP já vem com o ProLiant no HP SmartStart CD. A versão mais atual também está disponível em: http://www.hp.com/go/spp/download.

Para mais informações sobre o SPP, acesse: http://www.hp.com/go/spp ou http://www.hp.com/go/spp/documentation.

Os sistemas HP ProLiant que rodam Linux são compatíveis com Insight Management Agents (IM Agents), fornecidos através do SPP. Os IM Agents do SmartStart CD e/ou do SPP versão 7.1 e posterior são compatíveis com o Insight Remote Support.

Para ProLiants Linux suportados, o IM Agents versão 7.1 ou posterior deve estar instalado (ou verificado, se já instalado) no SPP para poder prosseguir.

Para verificar a versão do IM Agents instalada, execute este comando: **`rpm -q hp-snmp-agents`**

**Importante:** o suporte a SNMP (incluindo IM Agents e Drivers de integridade) não pode ocorrer no mesmo dispositivo monitorado que o WBEM (incluindo IM Providers e Drivers de integridade). O WBEM, se instalado, deve ser removido de acordo com a documentação do

SSP disponível em: http://www.hp.com/go/spp/documentation/.

**Observação:** No dispositivo monitorado Linux, o arquivo `/etc/snmp/snmpd.conf` contém informações de configuração SNMP. Durante o script de instalação dos IM Agents, procure informações sobre esse arquivo. Quando o script mostrar o prompt `Configuring SNMP access from remote Management Station(s)` (Configurar acesso SNMP a partir de estações de trabalho remotas), inclua o endereço de IP do dispositivo host. Se você não fizer isso, será preciso reconfigurar o SNMP.

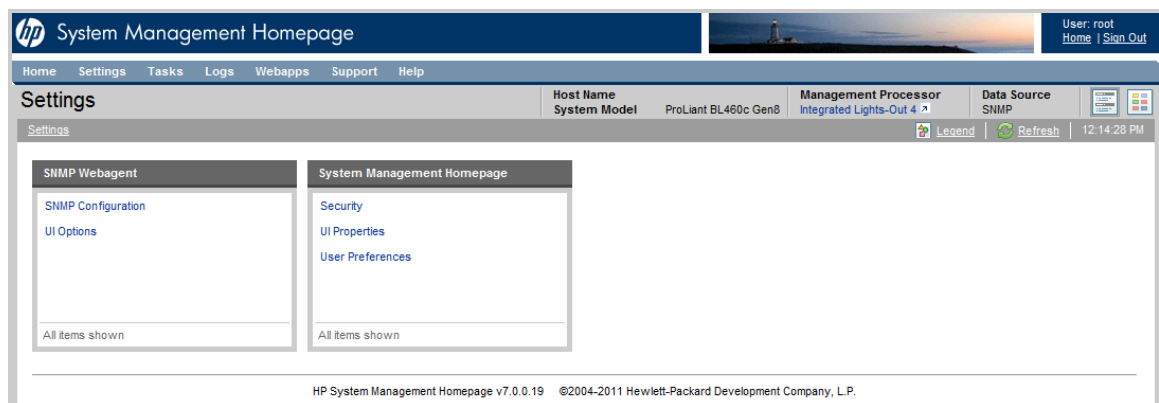
O System Management Homepage (SMH) também faz parte do SPP. Ele fornece recursos adicionais de relatório sobre o dispositivo monitorado. O SMH não é obrigatório para o Insight Remote Support, mas pode ser usado para reconfigurar o SNMP, caso as configurações feitas durante a instalação do Insight Management Agent precisem ser modificadas.

# Configurar o SNMP

Depois de instalar o Insight Management Agents nos dispositivos monitorados, use a SMH para editar o arquivo `snmpd.conf` para acrescentar o endereço de IP do dispositivo host e a cadeia de caracteres de comunidade SNMP. Isso possibilita a comunicação SNMP do dispositivo monitorado com o dispositivo host. Será preciso fazer isso para cada dispositivo Linux monitorado.

**Observação:** Você também pode editar o arquivo `snmpd.conf` em um editor de texto, se você não estiver usando a SMH.

O dispositivo host deve ser capaz de se comunicar com o dispositivo monitorado. Para configurar o dispositivo monitorado de forma a enviar interceptações ao dispositivo host, conclua as seguintes etapas:

1. Em um navegador, acesse o System Management Homepage (SMH) no dispositivo monitorado: `https://[`*`endereçoIP`*`]:2381`.
2. Faça login usando o nome de usuário raiz e a senha do dispositivo monitorado.
3. Na barra superior do menu, clique em **Configurações**.

4. Clique no link **Configuração SNMP**.
5. No arquivo de configuração SNMP, adicione uma entrada `trapsink` para o endereço de IP do

dispositivo host, por exemplo, `trapsink 1.2.3.4 public`, e clique em **Alterar**.

É preciso usar o comando `trapsink` para que os eventos sejam enviados ao Insight Remote Support para análise. Se o comando `trapsink` não for configurado, o Insight Remote Support não receberá interceptações.

Uma diretiva `rocommunity` permite acesso `SNMP GET` e `GETNEXT`. Ela é necessária para detecção e pelas regras de análise. O formato é: `rocommunity` <*community_string*>, por exemplo, `rocommunity public`. A cadeia de comunidade deve ser a mesma cadeia de caracteres de comunidade de leitura configurada no protocolo SNMP do Insight RS Console atribuída ao servidor ProLiant Linux. A `rocommunity` é usada durante o processamento de armadilhas de regras de análise para recuperar informações extras não fornecidas com as armadilhas.

A diretiva `rwcommunity` permite acesso `SNMP GET`, `GETNEXT` e `SET`. Ela não é obrigatória para o uso do Insight Remote Support, mas pode ser necessária para outros aplicativos.

**Observação:** Se você não usar a cadeia de caracteres de comunidade `public` na entrada `trapsink`, então precisará acrescentar um novo protocolo SNMP para esse dispositivo monitorado no Insight RS Console que usa a mesma cadeia de caracteres de comunidade.

6. Para as instalações no Linux (por exemplo: Red Hat 4 ou 5) compatíveis com a segurança extra de exibição de declarações, acrescente uma entrada `view systemview included` (exibição do sistema incluída). A entrada `view systemview included` permite que o Insight Remote Support leia toda a árvore .232 MIB e reúna todos os dados de análise quando eventos ocorrerem. Faça as seguintes alterações nas configurações padrão:

   a. Em **Arquivo de configuração SNMP**, localize as entradas `view systemview included` (exibição do sistema incluída).

b. Inclua comentários nas entradas padrão usando o caractere #.

c. Adicione a seguinte entrada: `view systemview included .1 80`

d. Clique em **Alterar**.

# Definir configurações de firewall e porta

Para obter uma lista completa de requisitos de firewall e de porta para dispositivos monitorados, consulte o *Informe de Segurança do HP Insight Remote Support*, em: http://www.hp.com/go/insightremotesupport/docs.

# Adicionar credenciais de protocolo e iniciar a detecção

Para detectar seus dispositivos monitorados, conclua as seguintes seções:

## Criar uma credencial de protocolo SNMP no Insight RS Console

Se a cadeia da comunidade SNMP do dispositivo estiver definida como `pública` e o modo de acesso da comunidade for `somente leitura`, o Insight RS associará automaticamente um protocolo SNMP ao seu dispositivo. Se você usar uma cadeia de comunidade diferente ou uma porta não padrão, precisará criar uma credencial de protocolo SNMP no Insight RS Console.

Para configurar o SNMP no Insight RS Console, conclua as seguintes etapas:

1. Em um navegador da Web, faça logon no Insight RS Console.
2. No menu principal, selecione **Detecção** e clique na guia **Credenciais**.

3. Na lista suspensa Selecionar e configurar protocolo:, selecione **Simple Network Management Protocol** para a versão do SNMP configurada no servidor.
4. Clique em **Novo**. A caixa de diálogo Nova credencial é exibida.
5. Digite as informações configuradas no seu servidor.
6. Clique em **Adicionar**.

O Insight RS cria a credencial de protocolo, que é exibida na tabela de credenciais.

## Detectar o dispositivo no Insight RS Console

Para detectar o dispositivo por meio do Insight RS Console, conclua as seguintes etapas:

1. Em um navegador da Web, faça logon no Insight RS Console.
2. No menu principal, selecione **Detecção** e clique na guia **Fontes**.
3. Expanda a seção Endereços IP e adicione o endereço IP do seu dispositivo:
   a. Clique em **Novo**.
   b. Selecione **Endereço único**, **Intervalo de endereços** ou **Lista de endereços**.
   c. Digite os endereços IP dos dispositivos a serem detectados.
   d. Clique em **Adicionar**.
4. Clique em **Iniciar detecção**.

## Verificar o status de detecção e do dispositivo

Para verificar se o dispositivo foi detectado corretamente, conclua as seguintes etapas:

1. Em um navegador da Web, faça logon no Insight RS Console.
2. No menu principal, selecione **Dispositivos** e clique na guia **Resumo do dispositivo**.
3. Verifique se a coluna Status contém um ícone de êxito ( ).

   Se não houver ícone de êxito, tente descobrir que coluna está com problema e consulte a Ajuda on-line para informações de solução de problemas.

# Verificar a comunicação entre o dispositivo monitorado e o Insight RS

Para verificar a comunicação entre o dispositivo monitorado e o Insight RS, conclua as seguintes seções:

# Verificar a conectividade enviando um teste de interceptação SNMP ao dispositivo host

Para verificar a conectividade do dispositivo monitorado com o dispositivo host, envie uma interceptação de teste SNMP ao dispositivo host e verifique se essa interceptação de teste foi recebida no Insight RS Console.

Use um dos seguintes métodos para enviar uma interceptação de teste SNMP ao dispositivo host.

- No SMH:
  a. Clique em **Configurações**.
  b. No painel SNMP Webagent, clique em **Configuração SNMP**.
  c. Vá até a parte de baixo da tela Configuração SNMP e, na seção Armadilha de teste, clique em **Enviar armadilha**.
- Na linha de comando, digite o seguinte comando para enviar uma interceptação de teste ao dispositivo host:

  **snmptrap -v 1 -c public [*endereço de IP do dispositivo host*] .1.3.6.1.4.1.232 [*endereço de IP do dispositivo monitorado no Linux*] 6 11003 1234 .1.3.6.1.2.1.1.5.0 s test .1.3.6.1.4.1.232.11.2.11.1.0 i 0 .1.3.6.1.4.1.232.11.2.8.1.0 s [*forneça seu próprio identificador e carimbo de hora]***

  Deve aparecer o resultado do teste, com detalhes sobre o dispositivo monitorado e o dispositivo host.

  ```
  Management Agents Test Trap sent - [carimbodehora]
  ```

# Visualizar eventos de teste no Insight RS Console

Alguns tipos de dispositivos monitorados permitem o envio de um evento de teste ao Insight Remote Support. Depois de configurar o dispositivo monitorado e enviar um evento de teste, use o seguinte processo para verificar se o evento de teste chegou.

1. Faça logon no Insight RS Console.
2. No menu principal, selecione **Eventos de serviços**. Se o dispositivo monitorado estiver configurado

adequadamente, o evento aparecerá no painel Informações sobre eventos de serviços.

# Verificar coletas no Insight RS Console

Coletas não são executadas automaticamente depois da descoberta. A HP recomenda que você execute uma coleta manualmente após a descoberta completa para verificar a conectividade. Execute o cronograma de coleta manualmente na guia Serviços de coleta → Agendamentos de coleta. Para obter mais informações sobre o agendamento de coletas, consulte a Ajuda do Insight RS.

Verifique se essa coleta foi bem-sucedida na guia Serviços de coleta → Resultados da coleta básica do Insight RS Console.

1. Faça logon no Insight RS Console.
2. No menu principal, selecione **Serviços de coleta** e depois clique na guia **Resultados da coleta básica**.
3. Expanda a seção Coleta de configurações básicas do servidor.
4. Localize a entrada referente ao seu dispositivo e verifique a coluna Resultado. Se a coleta tiver sido bem-sucedida, um ícone de êxito será exibido (). Se ocorrer uma falha, um ícone de erro será exibido ().

# Capítulo 5: Configurar servidores ProLiant VMware ESX

## Atender aos requisitos de configuração

Para configurar seus servidores ProLiant VMware ESX de forma que eles sejam monitorados pelo Insight RS, conclua as seguintes seções:

**Tabela 5.1** ***Etapas de configuração do servidor ProLiant VMware ESX***

| Tarefa | Concluída? |
|---|---|
| Certifique-se de que o Insight RS suporte seu servidor ProLiant VMware ESX, verificando o *Notas de Lançamento do HP Insight Remote Support*. | |
| Configure o SNMP no servidor ProLiant VMware ESX. | |
| Adicione as credenciais de protocolo do SNMP ao Insight RS Console. | |
| Detecte o servidor ProLiant VMware ESX no Insight RS Console. | |
| Envie um evento de teste para verificar a conectividade entre seu servidor ProLiant VMware ESX e o Insight RS. | |

## Instalar e configurar o software de comunicação em servidores

Para configurar seus dispositivos monitorados, conclua as seguintes seções:

## Configurar o SNMP

Os dispositivos monitorados devem ser configurados para se comunicar com o dispositivo host. O VMware ESX usa SNMP para comunicação com o dispositivo host. O SNMP deve ser instalado por padrão com o VMware ESX, mas você deve definir as configurações SNMP do dispositivo monitorado para comunicação com o dispositivo host.

Dispositivos monitorados que participam de notificações SNMP devem incluir o seguinte:

- Todos os dispositivos monitorados devem ter uma conexão de intranet em funcionamento, como através de um adaptador Ethernet, com o TCP/IP instalado e funcionando. Os dispositivos monitorados devem ter comunicação bidirecional com o dispositivo host através dessa conexão.
- Os dispositivos monitorados precisam do software Agente de gerenciamento para detecção de problemas e geração de interceptações. Os agentes IM são distribuídos pela HP e projetados para gerar interceptações SNMP com informações que possibilitam uma análise mais completa. Com o VMware ESX, os agentes de gerenciamento fazem parte do pacote do VMware ESX. Assim, se seu dispositivo monitorado estiver configurado corretamente, os agentes estarão presentes no servidor.
- Por fim, todos os dispositivos monitorados precisam ter o endereço IP do dispositivo host definido como um destino de interceptação.

Os agentes SNMP são necessários para dispositivos monitorados no VMware ESX. Depois de instalar os agentes SNMP nos dispositivos monitorados, use a SMH para editar o arquivo `snmpd.conf` para acrescentar o endereço de IP do dispositivo host e a cadeia de caracteres de comunidade SNMP. Isso possibilita a comunicação SNMP do dispositivo monitorado com o dispositivo host. Será preciso fazer isso para cada dispositivo monitorado no VMware ESX.

**Observação:** Você também pode editar o arquivo `snmpd.conf` em um editor de texto, se você não estiver usando a SMH.

O dispositivo host deve ser capaz de se comunicar com o dispositivo monitorado. Para configurar o dispositivo monitorado de forma a enviar interceptações ao dispositivo host, conclua as seguintes etapas:

1. Em um navegador, acesse o System Management Homepage (SMH) no dispositivo monitorado: `https://[`*`endereçoIP`*`]:2381`.
2. Faça login usando o nome do usuário raiz e a senha do dispositivo monitorado.
3. Na barra superior do menu, clique em **Configurações**.

4. Clique no link **Configuração SNMP**.
5. No arquivo de configuração SNMP, adicione um comando `trapsink` que inclua o endereço de IP do dispositivo host; por exemplo: `trapsink 1.2.3.4 public`, e clique em **Alterar**.

   É preciso usar o comando `trapsink` para que os eventos sejam enviados ao Insight Remote Support para análise. Se o comando `trapsink` não for configurado, o Insight Remote Support não receberá interceptações.

   Uma diretiva `rocommunity` permite acesso `SNMP GET` e `GETNEXT`. Ela é necessária para detecção e pelas regras de análise. O formato é: `rocommunity` *`<community_string>`*, por exemplo, `rocommunity public`. A cadeia de comunidade deve ser a mesma cadeia de caracteres de comunidade de leitura configurada no protocolo SNMP do Insight RS Console atribuída ao servidor ProLiant ESX. A `rocommunity` é usada durante o processamento de armadilhas de regras de análise para recuperar informações extras não fornecidas com as armadilhas.

   A diretiva `rwcommunity` permite acesso `SNMP GET`, `GETNEXT` e `SET`. Ela não é obrigatória para o uso do Insight Remote Support, mas pode ser necessária para outros aplicativos.

**Observação:** Se você não usar a cadeia de caracteres de comunidade `public` na entrada `trapsink`, então precisará acrescentar um novo protocolo SNMP para esse dispositivo

monitorado no Insight RS Console que usa a mesma cadeia de caracteres de comunidade.

6. Para as instalações no Linux (por exemplo: Red Hat 4 ou 5) compatíveis com a segurança extra de exibição de declarações, acrescente uma entrada `view systemview included` (exibição do sistema incluída). A entrada `view systemview included` permite que o Insight Remote Support leia toda a árvore .232 MIB e reúna todos os dados de análise quando eventos ocorrerem. Faça as seguintes alterações nas configurações padrão:

   a. Em **Arquivo de configuração SNMP**, localize as entradas `view systemview included` (exibição do sistema incluída).

b. Inclua comentários nas entradas padrão usando o caractere #.

c. Adicione a seguinte entrada: `view systemview included .1 80`

d. Clique em **Alterar**.

# Definir configurações de firewall e porta

Para obter uma lista completa de requisitos de firewall e de porta para dispositivos monitorados, consulte o *Informe de Segurança do HP Insight Remote Support*, em: http://www.hp.com/go/insightremotesupport/docs.

## Adicionar credenciais de protocolo e iniciar a detecção

Para detectar seus dispositivos monitorados, conclua as seguintes seções:

### Criar uma credencial de protocolo SNMP no Insight RS Console

Se a cadeia da comunidade SNMP do dispositivo estiver definida como `pública` e o modo de acesso da comunidade for `somente leitura`, o Insight RS associará automaticamente um protocolo SNMP ao seu dispositivo. Se você usar uma cadeia de comunidade diferente ou uma porta não padrão, precisará criar uma credencial de protocolo SNMP no Insight RS Console.

Para configurar o SNMP no Insight RS Console, conclua as seguintes etapas:

1. Em um navegador da Web, faça logon no Insight RS Console.
2. No menu principal, selecione **Detecção** e clique na guia **Credenciais**.
3. Na lista suspensa Selecionar e configurar protocolo:, selecione **Simple Network Management Protocol** para a versão do SNMP configurada no servidor.
4. Clique em **Novo**. A caixa de diálogo Nova credencial é exibida.

5. Digite as informações configuradas no seu servidor.
6. Clique em **Adicionar**.

O Insight RS cria a credencial de protocolo, que é exibida na tabela de credenciais.

Detectar o dispositivo no Insight RS Console

Para detectar o dispositivo por meio do Insight RS Console, conclua as seguintes etapas:

1. Em um navegador da Web, faça logon no Insight RS Console.
2. No menu principal, selecione **Detecção** e clique na guia **Fontes**.
3. Expanda a seção Endereços IP e adicione o endereço IP do seu dispositivo:
   a. Clique em **Novo**.
   b. Selecione **Endereço único**, **Intervalo de endereços** ou **Lista de endereços**.
   c. Digite os endereços IP dos dispositivos a serem detectados.
   d. Clique em **Adicionar**.
4. Clique em **Iniciar detecção**.

Verificar o status de detecção e do dispositivo

Para verificar se o dispositivo foi detectado corretamente, conclua as seguintes etapas:

1. Em um navegador da Web, faça logon no Insight RS Console.
2. No menu principal, selecione **Dispositivos** e clique na guia **Resumo do dispositivo**.
3. Verifique se a coluna Status contém um ícone de êxito ( ).

   Se não houver ícone de êxito, tente descobrir que coluna está com problema e consulte a Ajuda on-line para informações de solução de problemas.

# Verificar a comunicação entre o dispositivo monitorado e o Insight RS

Para verificar a comunicação entre o dispositivo monitorado e o Insight RS, conclua as seguintes seções:

## Verificar a conectividade enviando um teste de interceptação SNMP ao dispositivo host

Para verificar a conectividade do dispositivo monitorado com o dispositivo host, envie uma interceptação de teste SNMP ao dispositivo host e verifique se essa interceptação de teste foi recebida no Insight RS Console.

Use um dos seguintes métodos para enviar uma interceptação de teste SNMP ao dispositivo host.

- No SMH:
  a. Clique em **Configurações**.
  b. No painel SNMP Webagent, clique em **Configuração SNMP**.
  c. Vá até a parte de baixo da tela Configuração SNMP e, na seção Armadilha de teste, clique em **Enviar armadilha**.
- Na linha de comando, digite o seguinte comando para enviar uma interceptação de teste ao dispositivo host:

  **snmptrap -v 1 -c public [*endereço de IP do dispositivo host*] .1.3.6.1.4.1.232 [*endereço de IP do dispositivo monitorado no Linux*] 6 11003 1234 .1.3.6.1.2.1.1.5.0 s test .1.3.6.1.4.1.232.11.2.11.1.0 i 0 .1.3.6.1.4.1.232.11.2.8.1.0 s [*forneça seu próprio identificador e carimbo de hora*]**

  Deve aparecer o resultado do teste, com detalhes sobre o dispositivo monitorado e o dispositivo host.

  ```
  Management Agents Test Trap sent - [carimbodehora]
  ```

# Visualizar eventos de teste no Insight RS Console

Alguns tipos de dispositivos monitorados permitem o envio de um evento de teste ao Insight Remote Support. Depois de configurar o dispositivo monitorado e enviar um evento de teste, use o seguinte processo para verificar se o evento de teste chegou.

1. Faça logon no Insight RS Console.
2. No menu principal, selecione **Eventos de serviços**. Se o dispositivo monitorado estiver configurado adequadamente, o evento aparecerá no painel Informações sobre eventos de serviços.

# Verificar coletas no Insight RS Console

Coletas não são executadas automaticamente depois da descoberta. A HP recomenda que você execute uma coleta manualmente após a descoberta completa para verificar a conectividade. Execute o cronograma de coleta manualmente na guia Serviços de coleta → Agendamentos de coleta. Para obter mais informações sobre o agendamento de coletas, consulte a Ajuda do Insight RS.

Verifique se essa coleta foi bem-sucedida na guia Serviços de coleta → Resultados da coleta básica do Insight RS Console.

1. Faça logon no Insight RS Console.
2. No menu principal, selecione **Serviços de coleta** e depois clique na guia **Resultados da coleta básica**.
3. Expanda a seção Coleta de configurações básicas do servidor.
4. Localize a entrada referente ao seu dispositivo e verifique a coluna Resultado. Se a coleta tiver sido bem-sucedida, um ícone de êxito será exibido (). Se ocorrer uma falha, um ícone de erro será exibido ().

# Capítulo 6: Configurar servidores ProLiant VMware ESXi

## Atender aos requisitos de configuração

Para configurar seus servidores ProLiant VMware ESXi de forma que eles sejam monitorados pelo Insight RS, conclua as seguintes seções:

**Tabela 6.1** ***Etapas de configuração do servidor ProLiant VMware ESXi***

| Tarefa | Concluída? |
|---|---|
| Certifique-se de que o Insight RS suporte seu servidor ProLiant VMware ESXi, verificando o *Notas de Lançamento do HP Insight Remote Support*. | |
| Instale e configure os provedores WBEM no servidor ESXi. Se estiver usando a imagem HP ESXi, todos os provedores WBEM necessários estarão incluídos. | |
| Adicione as credenciais de protocolo do WBEM ao Insight RS Console. | |
| Detecte o servidor ProLiant VMware ESXi no Insight RS Console. | |
| Verifique a comunicação entre o servidor ESXi e o Insight RS. | |

## Instalar e configurar o software de comunicação em servidores

Para configurar seus dispositivos monitorados, conclua as seguintes seções:

## Instalar uma imagem ESXi

Existem dois métodos de obtenção do ESXi:

- Use a imagem HP ESXi, que contém os provedores de WBEM e o Pacote de utilitários (consulte "Obter a imagem HP ESXi").
- Use a imagem VMware ESXi, que não contém os provedores WBEM ou o Pacote de utilitários. Os provedores WBEM e o Pacote de utilitários precisam ser instalados separadamente e também são disponibilizados pela HP (consulte "Obter pacotes para configurar a imagem VMware ESXi").

### *Obter a imagem HP ESXi*

A imagem HP ESXi inclui os provedores WBEM necessários para enviar eventos de hardware ao dispositivo host. Use as credenciais da conta raiz para o sistema ESXi quando for configurar os protocolos WBEM para esse dispositivo monitorado no dispositivo host. A capacidade de enviar um evento de teste é habilitada pelo Utilitário de eventos de teste, que faz parte do Pacote de utilitários ESXi incluído na imagem HP ESXi.

**Importante:** Se estiver usando a imagem HP ESXi, não será necessário baixar e instalar o

pacote de provedores WBEM, pois a imagem já terá o pacote integrado.

Baixe a imagem ESXi da HP no seguinte link:

www.hp.com/go/esxidownload

### Obter pacotes para configurar a imagem VMware ESXi

A HP desenvolveu provedores WBEM para VMware ESXi. O pacote contém os provedores WBEM, e é preciso baixar e instalar o pacote quando a imagem usada para instalar o sistema operacional ESXi tiver sido fornecida pela VMware. Para enviar eventos de teste, você também deve instalar o Pacote de utilitários HP ESXi, que inclui o utilitário de evento teste.

Baixe os Pacotes Offline e o Pacote de utilitários HP ESXi no seguinte link:

www.hp.com/go/esxidownload

## Definir configurações de firewall e porta

Para obter uma lista completa de requisitos de firewall e de porta para dispositivos monitorados, consulte o *Informe de Segurança do HP Insight Remote Support*, em: http://www.hp.com/go/insightremotesupport/docs.

# Adicionar credenciais de protocolo e iniciar a detecção

**Importante:** Se você estiver gerenciando seus hosts ESXi usando o servidor VMware vCenter, poderá ignorar as etapas a seguir e detectar todos os hosts ESXi com uma única detecção do servidor VMware vCenter. Para obter mais informações, consulte "Configurar servidores VMware vCenter".

Para detectar seus dispositivos monitorados, conclua as seguintes seções:

## Criar uma credencial de protocolo WBEM no Insight RS Console

Para configurar o WBEM no Insight RS Console, conclua as seguintes etapas:

1. Em um navegador da Web, faça logon no Insight RS Console.
2. No menu principal, selecione **Detecção** e clique na guia **Credenciais**.
3. Na lista suspensa **Selecionar e configurar protocolo**, selecione **Gerenciamento Corporativo baseado na Web (WBEM)**.
4. Clique em **Novo**. A caixa de diálogo Nova credencial é exibida.
5. Digite o nome de usuário e a senha configurados no seu dispositivo.
6. Clique em **Adicionar**.

O Insight RS cria a credencial de protocolo, que é exibida na tabela de credenciais.

# Detectar o dispositivo no Insight RS Console

Para detectar o dispositivo por meio do Insight RS Console, conclua as seguintes etapas:

1. Em um navegador da Web, faça logon no Insight RS Console.
2. No menu principal, selecione **Detecção** e clique na guia **Fontes**.
3. Expanda a seção Endereços IP e adicione o endereço IP do seu dispositivo:
    a. Clique em **Novo**.
    b. Selecione **Endereço único**, **Intervalo de endereços** ou **Lista de endereços**.
    c. Digite os endereços IP dos dispositivos a serem detectados.
    d. Clique em **Adicionar**.
4. Clique em **Iniciar detecção**.

# Verificar o status de detecção e do dispositivo

Para verificar se o dispositivo foi detectado corretamente, conclua as seguintes etapas:

1. Em um navegador da Web, faça logon no Insight RS Console.
2. No menu principal, selecione **Dispositivos** e clique na guia **Resumo do dispositivo**.
3. Verifique se a coluna Status contém um ícone de êxito ( ).

    Se não houver ícone de êxito, tente descobrir que coluna está com problema e consulte a Ajuda on-line para informações de solução de problemas.

# Verificar a comunicação entre o dispositivo monitorado e o Insight RS

Para verificar a comunicação entre o dispositivo monitorado e o Insight RS, conclua a seguinte seção:

# Verificar a conectividade enviando um evento de teste para o dispositivo host

O Utilitário de evento de testes do ESXi permite enviar eventos-teste ao dispositivo host. Esse utilitário está disponível para o VMware ESXi 5.0, o VMware vSphere® e o vSphere 5.5 e versões posteriores.

Para obter mais informações sobre como usar o Utilitário de eventos de teste, consulte o *Guia do Usuário para Utilitários HP VMware*.

**Importante:** Se você estiver usando a imagem VMware ESXi, deverá instalar o Pacote offline

de utilitários ESXi para enviar eventos de teste. Consulte "Obter pacotes para configurar a imagem VMware ESXi".

No dispositivo monitorado, use um dos seguintes métodos para executar o comando `hptestevent`:

- Execute o comando diretamente no host ESXi:

  **`/opt/hp/tools/hptestevent`**

- Use esxcli para executar o comando:

  **`esxcli hptestevent execute`**

# Visualizar eventos de teste no Insight RS Console

Alguns tipos de dispositivos monitorados permitem o envio de um evento de teste ao Insight Remote Support. Depois de configurar o dispositivo monitorado e enviar um evento de teste, use o seguinte processo para verificar se o evento de teste chegou.

1. Faça logon no Insight RS Console.
2. No menu principal, selecione **Eventos de serviços**. Se o dispositivo monitorado estiver configurado adequadamente, o evento aparecerá no painel Informações sobre eventos de serviços.

# Verificar coletas no Insight RS Console

Coletas não são executadas automaticamente depois da descoberta. A HP recomenda que você execute uma coleta manualmente após a descoberta completa para verificar a conectividade. Execute o cronograma de coleta manualmente na guia Serviços de coleta → Agendamentos de coleta. Para obter mais informações sobre o agendamento de coletas, consulte a Ajuda do Insight RS.

Verifique se essa coleta foi bem-sucedida na guia Serviços de coleta → Resultados da coleta básica do Insight RS Console.

1. Faça logon no Insight RS Console.
2. No menu principal, selecione **Serviços de coleta** e depois clique na guia **Resultados da coleta básica**.
3. Expanda a seção Coleta de configurações básicas do servidor.

4. Localize a entrada referente ao seu dispositivo e verifique a coluna Resultado. Se a coleta tiver sido bem-sucedida, um ícone de êxito será exibido ( ). Se ocorrer uma falha, um ícone de erro será exibido ( ).

# Capítulo 7: Configurar ProLiant Citrix XenServers

## Atender aos requisitos de configuração

Para configurar seus ProLiant Citrix XenServeres de forma que eles sejam monitorados pelo Insight RS, conclua as seguintes seções:

**Tabela 7.1** ***Etapas de configuração do ProLiant Citrix XenServer***

| Tarefa | Concluída? |
|---|---|
| Verifique se o Insight RS oferece suporte ao seu ProLiant Citrix XenServer consultando o documento *Notas de Lançamento do HP Insight Remote Support*. | |
| Instale agentes SNMP HP para Citrix XenServer no ProLiant Citrix XenServer. | |
| Configure o SNMP no ProLiant Citrix XenServer. | |
| Adicione o protocolo SNMP ao Insight RS Console. | |
| Detecte o servidor ProLiant Citrix no Insight RS Console. | |
| Envie um evento de teste para verificar a conectividade entre o ProLiant Citrix XenServer e o Insight RS. | |

## Instalar e configurar o software de comunicação em servidores

Para configurar seus dispositivos monitorados, conclua as seguintes seções:

## Instalar agentes SNMP para o Citrix XenServer

Os dispositivos monitorados no Citrix devem ser configurados para se comunicar com o dispositivo host. Dispositivos monitorados que usam notificações SNMP devem incluir o seguinte:

- Todos os dispositivos monitorados devem ter uma conexão de intranet em funcionamento, como através de um adaptador Ethernet, com o TCP/IP instalado e funcionando. Os dispositivos monitorados devem ter comunicação bidirecional com o dispositivo host através dessa conexão.
- Os dispositivos monitorados precisam do software agente SNMP para detecção de problemas e geração de armadilhas. A HP distribui os agentes SNMP, e eles foram projetados para gerar armadilhas SNMP com informações que possibilitam uma análise mais completa.
- Por fim, todos os dispositivos monitorados precisam ter o endereço IP do dispositivo host definido como um destino de interceptação.

Os agentes SNMP HP para Citrix XenServer constituem um pacote de software específico de sistema que inclui drivers, utilitários e agentes de gerenciamento para o Citrix ProLiant. Os agentes SNMP HP para Citrix XenServer podem ser encontrados no seguinte link: http://h20000.www2.hp.com/bizsupport/TechSupport/SoftwareDescription.jsp?swItem=MTX-9f349b2b4fc94915ac6cde8b8a.

Os agentes SNMP suportam sistemas HP ProLiant que executam Citrix, os quais vêm incluídos no pacote do software dos agentes SNMP HP para Citrix XenServer.

**Observação:** No dispositivo monitorado no Citrix, o arquivo `/etc/snmp/snmpd.conf` contém a configuração SNMP atual. Durante a configuração do script de instalação dos agentes SNMP, veja as informações sobre esse arquivo. Quando o script mostrar o prompt `Configuring SNMP access from remote Management Station(s)` (Configurar acesso SNMP a partir de estações de trabalho remotas), inclua o endereço de IP do dispositivo host. Se você não incluir, terá de reconfigurar o endereço no dispositivo monitorado.

A Página Inicial do Gerenciamento de Sistemas (SMH) também vem no pacote de software dos agentes SNMP HP para Citrix XenServer. Ele fornece recursos adicionais de relatório sobre o dispositivo monitorado. Embora não seja obrigatório para o Insight Remote Support, se você configurar os serviços SNMP incorretamente para se comunicar com o dispositivo host durante a instalação dos agentes SNMP, será preciso que a SMH refaça essas configurações.

# Configurar o SNMP

Os agentes SNMP são necessários para dispositivos monitorados no Citrix. Depois de instalar os agentes SNMP nos dispositivos monitorados, use a SMH para editar o arquivo `snmpd.conf` para acrescentar o endereço de IP do dispositivo host e a cadeia de caracteres de comunidade SNMP. Isso possibilita a comunicação SNMP do dispositivo monitorado com o dispositivo host. Será preciso fazer isso para cada dispositivo monitorado no Citrix.

**Observação:** Você também pode editar o arquivo `snmpd.conf` em um editor de texto, se você não estiver usando a SMH.

O dispositivo host deve ser capaz de se comunicar com o dispositivo monitorado. Para configurar o dispositivo monitorado de forma a enviar interceptações ao dispositivo host, conclua as seguintes etapas:

1. Em um navegador, acesse o System Management Homepage (SMH) no dispositivo monitorado: `https://[`*`endereçoIP`*`]:2381`.
2. Faça login usando o nome do usuário raiz e a senha do dispositivo monitorado.
3. Na barra superior do menu, clique em **Configurações**.

4. Clique no link **Configuração SNMP**.
5. No arquivo de configuração SNMP, adicione um comando `trapsink` que inclua o endereço de IP do dispositivo host; por exemplo: `trapsink 1.2.3.4 public`, e clique em **Alterar**.

   É preciso usar o comando `trapsink` para que os eventos sejam enviados ao Insight Remote Support para análise. Se o comando `trapsink` não for configurado, o Insight Remote Support não receberá interceptações.

   Uma diretiva `rocommunity` permite acesso `SNMP GET` e `GETNEXT`. Ela é necessária para detecção e pelas regras de análise. O formato é: `rocommunity` *<community_string>*, por exemplo, `rocommunity public`. A cadeia de comunidade deve ser a mesma cadeia de caracteres de comunidade de leitura configurada no protocolo SNMP do Insight RS Console atribuída ao servidor ProLiant Citrix. A `rocommunity` é usada durante o processamento de armadilhas de regras de análise para recuperar informações extras não fornecidas com as armadilhas.

   A diretiva `rwcommunity` permite acesso `SNMP GET`, `GETNEXT` e `SET`. Ela não é obrigatória para o uso do Insight Remote Support, mas pode ser necessária para outros aplicativos.

**Observação:** Se você não usar a cadeia de caracteres de comunidade `public` na entrada `trapsink`, então precisará acrescentar um novo protocolo SNMP para esse dispositivo monitorado no Insight RS Console que usa a mesma cadeia de caracteres de comunidade.

6. Para as instalações no Linux (por exemplo: Red Hat 4 ou 5) compatíveis com a segurança extra de exibição de declarações, acrescente uma entrada `view systemview included` (exibição do sistema incluída). A entrada `view systemview included` permite que o Insight Remote Support leia toda a árvore .232 MIB e reúna todos os dados de análise quando eventos ocorrerem. Faça as seguintes alterações nas configurações padrão:

   a. Em **Arquivo de configuração SNMP**, localize as entradas `view systemview included` (exibição do sistema incluída).

b. Inclua comentários nas entradas padrão usando o caractere #.

c. Adicione a seguinte entrada: `view systemview included .1 80`

d. Clique em **Alterar**.

# Definir configurações de firewall e porta

Para obter uma lista completa de requisitos de firewall e de porta para dispositivos monitorados, consulte o *Informe de Segurança do HP Insight Remote Support*, em: http://www.hp.com/go/insightremotesupport/docs.

### Adicionar credenciais de protocolo e iniciar a detecção

Para detectar seus dispositivos monitorados, conclua as seguintes seções:

### Criar uma credencial de protocolo SNMP no Insight RS Console

Se a cadeia da comunidade SNMP do dispositivo estiver definida como `pública` e o modo de acesso da comunidade for `somente leitura`, o Insight RS associará automaticamente um protocolo SNMP ao seu dispositivo. Se você usar uma cadeia de comunidade diferente ou uma porta não padrão, precisará criar uma credencial de protocolo SNMP no Insight RS Console.

Para configurar o SNMP no Insight RS Console, conclua as seguintes etapas:

1. Em um navegador da Web, faça logon no Insight RS Console.
2. No menu principal, selecione **Detecção** e clique na guia **Credenciais**.
3. Na lista suspensa Selecionar e configurar protocolo:, selecione **Simple Network Management Protocol** para a versão do SNMP configurada no servidor.
4. Clique em **Novo**. A caixa de diálogo Nova credencial é exibida.

5. Digite as informações configuradas no seu servidor.
6. Clique em **Adicionar**.

O Insight RS cria a credencial de protocolo, que é exibida na tabela de credenciais.

Detectar o dispositivo no Insight RS Console

Para detectar o dispositivo por meio do Insight RS Console, conclua as seguintes etapas:

1. Em um navegador da Web, faça logon no Insight RS Console.
2. No menu principal, selecione **Detecção** e clique na guia **Fontes**.
3. Expanda a seção Endereços IP e adicione o endereço IP do seu dispositivo:
   a. Clique em **Novo**.
   b. Selecione **Endereço único**, **Intervalo de endereços** ou **Lista de endereços**.
   c. Digite os endereços IP dos dispositivos a serem detectados.
   d. Clique em **Adicionar**.
4. Clique em **Iniciar detecção**.

Verificar o status de detecção e do dispositivo

Para verificar se o dispositivo foi detectado corretamente, conclua as seguintes etapas:

1. Em um navegador da Web, faça logon no Insight RS Console.
2. No menu principal, selecione **Dispositivos** e clique na guia **Resumo do dispositivo**.
3. Verifique se a coluna Status contém um ícone de êxito ().

   Se não houver ícone de êxito, tente descobrir que coluna está com problema e consulte a Ajuda on-line para informações de solução de problemas.

# Verificar a comunicação entre o dispositivo monitorado e o Insight RS

Para verificar a comunicação entre o dispositivo monitorado e o Insight RS, conclua as seguintes seções:

# Verificar a conectividade enviando um teste de interceptação SNMP ao dispositivo host

Para verificar a conectividade do dispositivo monitorado com o dispositivo host, envie uma interceptação de teste SNMP ao dispositivo host e verifique se essa interceptação de teste foi recebida no Insight RS Console.

Use um dos seguintes métodos para enviar uma interceptação de teste SNMP ao dispositivo host.

- No SMH:
    a. Clique em **Configurações**.
    b. No painel SNMP Webagent, clique em **Configuração SNMP**.
    c. Vá até a parte de baixo da tela Configuração SNMP e, na seção Armadilha de teste, clique em **Enviar armadilha**.
- Na linha de comando, digite o seguinte comando para enviar uma interceptação de teste ao dispositivo host:

```
snmptrap -v 1 -c public [endereço de IP do dispositivo host] .1.3.6.1.4.1.232
[endereço de IP do dispositivo monitorado no Linux] 6 11003 1234 .1.3.6.1.2.1.1.5.0
s test .1.3.6.1.4.1.232.11.2.11.1.0 i 0 .1.3.6.1.4.1.232.11.2.8.1.0 s [forneça seu
próprio identificador e carimbo de hora]
```

  Deve aparecer o resultado do teste, com detalhes sobre o dispositivo monitorado e o dispositivo host.

```
Management Agents Test Trap sent - [carimbodehora]
```

# Visualizar eventos de teste no Insight RS Console

Alguns tipos de dispositivos monitorados permitem o envio de um evento de teste ao Insight Remote Support. Depois de configurar o dispositivo monitorado e enviar um evento de teste, use o seguinte processo para verificar se o evento de teste chegou.

1. Faça logon no Insight RS Console.
2. No menu principal, selecione **Eventos de serviços**. Se o dispositivo monitorado estiver configurado adequadamente, o evento aparecerá no painel Informações sobre eventos de serviços.

# Verificar coletas no Insight RS Console

Coletas não são executadas automaticamente depois da descoberta. A HP recomenda que você execute uma coleta manualmente após a descoberta completa para verificar a conectividade. Execute o cronograma de coleta manualmente na guia Serviços de coleta → Agendamentos de coleta. Para obter mais informações sobre o agendamento de coletas, consulte a Ajuda do Insight RS.

Verifique se essa coleta foi bem-sucedida na guia Serviços de coleta → Resultados da coleta básica do Insight RS Console.

1. Faça logon no Insight RS Console.
2. No menu principal, selecione **Serviços de coleta** e depois clique na guia **Resultados da coleta básica**.
3. Expanda a seção Coleta de configurações básicas do servidor.
4. Localize a entrada referente ao seu dispositivo e verifique a coluna Resultado. Se a coleta tiver sido bem-sucedida, um ícone de êxito será exibido (). Se ocorrer uma falha, um ícone de erro será exibido ().

# Capítulo 8: Configurar servidores Integrity Windows 2003

O Coletor de Monitoramento do Log de Eventos (ELMC) é responsável pelo monitoramento do suporte remoto nos dispositivos monitorados Integrity Windows 2003. O SNMP é necessário para detecção, e o WBEM é necessário para coleta de configurações.

## Atender aos requisitos de configuração

Para configurar servidores Integrity Windows 2003 de forma que eles sejam monitorados pelo Insight RS, conclua as seguintes seções:

**Tabela 8.1** ***Etapas de configuração do servidor Integrity Windows 2003***

| Tarefa | Concluída? |
|---|---|
| Certifique-se de que o Insight RS suporte seu servidor Integrity Windows 2003, verificando o *Notas de Lançamento do HP Insight Remote Support*. | |
| Instale o ELMC no servidor Integrity Windows 2003. | |
| Verifique se o SNMP está instalado no servidor Integrity Windows 2003. | |
| Verifique se o WBEM está instalado no servidor Integrity Windows 2003. | |
| Adicione o protocolo ELMC ao Insight RS Console. | |
| Adicione o protocolo SNMP ao Insight RS Console. | |
| Adicione o protocolo WBEM ao Insight RS Console. | |
| Detecte o servidor Integrity Windows 2003 no Insight RS Console. | |
| Envie um evento de teste para verificar a conectividade entre seu servidor Integrity Windows 2003 e o Insight RS. | |

## Instalar e configurar o software de comunicação em servidores

Para configurar seus dispositivos monitorados, conclua as seguintes seções:

### Instalar o pacote de software do ELMC no dispositivo monitorado

O dispositivo monitorado deve atender às seguintes exigências básicas para que você instale o ELMC:

- Arquitetura do processador: Itanium nos servidores Integrity
- Sistema operacional: nos servidores Integrity, todas as versões aceitas do Windows 2003
- TCP-IP configurado no servidor monitorado

- Permissões e acesso necessários: para instalar, atualizar ou desinstalar o ELMC, você precisa se registrar como Administrador ou como usuário com privilégios de administrador.

O ELMC é necessário no servidor Integrity Windows 2003 para que os eventos possam ser encaminhados para o Insight RS.

Se o ELMC já estiver instalado no servidor Integrity Windows 2003, certifique-se de que sua versão seja a 6.2 ou posterior. Se a versão for anterior à 6.2, será preciso atualizá-la. Para verificar a versão do ELMC, execute o seguinte comando:`wccproxy version`.

**Observação:** Ao atualizar para o ELMC versão 6.4, o número de versão incorreto é mostrado na janela de atualização. Após a execução da atualização, o número de versão correto 6.4 aparecerá na janela Programas e recursos e quando você executar o comando `wccproxy version`.

Para instalar o pacote de software do ELMC, conclua as seguintes etapas:

1. No Insight RS Console, navegue até a guia **Configurações do administrador** → **Atualizações de software** e selecione o pacote de software *Coletor de Monitoramento do Log de Eventos (ELMC)*.
2. Na guia **Versão disponível**, clique em **Download**.
3. Quando o download for concluído, clique em **Instalar**. Os pacotes do ELMC são guardados na pasta `%HP_RS_DATA%\ELMC`. Por padrão, a pasta é `C:\ProgramData\HP\RS\DATA\ELMC`.

   **Observação**: A pasta `ProgramData` é uma pasta oculta. Para exibir essa pasta, defina as opções de pasta para mostrar pastas ocultas.
4. Copie o pacote de software apropriado do ELMC para Itanium (IA64) ou x86/x64 para um diretório temporário no servidor Integrity Windows 2003.
5. Dê um clique duplo no arquivo do instalador para iniciar o processo de instalação. O kit será instalado e encerrado sem prompts ao usuário. Não é necessário entrar com nenhuma configuração de usuário para instalar o pacote de software do ELMC.

# Verificar pré-requisitos do agente SNMP no dispositivo monitorado

Para o dispositivo Integrity Windows 2003 a ser monitorado pelo Insight RS Console, é necessário que os agentes SNMP do HP Integrity para o Windows Server 2003 estejam instalados e devidamente configurados nos dispositivos monitorados, conforme as instruções que constam na documentação do produto HP Smart Setup no respectivo pacote.

**Observação:** os provedores WBEM podem coexistir com agentes SNMP no sistema do dispositivo monitorado, contanto que tenham o mesmo número de versão. Não há compatibilidade para versões diferentes dos provedores de WBEM do HP Insight Management e dos agentes SNMP do HP Insight Management.

Os servidores Integrity Windows fabricados pela HP já acompanham os arquivos de instalação Smart Setup pré-carregados no disco do sistema operacional. Nos demais casos, os pacotes podem ser instalados usando o CD Smart Setup ou a mídia de reinstalação. Você pode baixar o CD Smart Setup ou

o Integrity Support Pack em:
http://h20000.www2.hp.com/bizsupport/TechSupport/SoftwareIndex.jsp?lang=en&cc=us&prodNameId=3346453&prodTypeId=15351&prodSeriesId=3346452&swLang=13&taskId=135&swEnvOID=1060.

Para que os agentes SNMP se comuniquem com o dispositivo host, você precisa fornecer as credenciais de SNMP dentro do Insight RS Console. Esse procedimento deverá ser realizado dentro do Insight RS Console no dispositivo host quando você estiver concluindo a configuração do Insight Remote Support.

# Verificar pré-requisitos do provedor WBEM no dispositivo monitorado

Para que o dispositivo Integrity Windows 2003 a ser monitorado seja compatível com coleta de configuração, é necessário que os provedores WBEM do HP Integrity para Windows Server 2003 estejam instalados e devidamente configurados nos dispositivos monitorados, conforme as instruções que constam na documentação do produto HP Smart Setup no respectivo pacote.

**Observação:** os provedores WBEM podem coexistir com agentes SNMP no sistema do dispositivo monitorado, contanto que tenham o mesmo número de versão. Não há compatibilidade para versões diferentes dos provedores de WBEM do HP Insight Management e dos agentes SNMP do HP Insight Management.

Os servidores Integrity Windows fabricados pela HP já acompanham os arquivos de instalação Smart Setup pré-carregados no disco do sistema operacional. Nos demais casos, os pacotes podem ser instalados usando o CD Smart Setup ou a mídia de reinstalação. Você pode baixar o CD Smart Setup ou o Integrity Support Pack em:
http://h20000.www2.hp.com/bizsupport/TechSupport/SoftwareIndex.jsp?lang=en&cc=us&prodNameId=3346453&prodTypeId=15351&prodSeriesId=3346452&swLang=13&taskId=135&swEnvOID=1060.

Para que os provedores WBEM se comuniquem com o dispositivo host, você precisa fornecer as credenciais WBEM, conforme instruções em *Guia de Instalação e Configuração do HP Insight Remote Support*. Esse procedimento deverá ser realizado dentro do Insight RS Console quando você estiver concluindo a configuração do Insight Remote Support.

# Definir configurações de firewall e porta

Para obter uma lista completa de requisitos de firewall e de porta para dispositivos monitorados, consulte o *Informe de Segurança do HP Insight Remote Support*, em:
http://www.hp.com/go/insightremotesupport/docs.

# Adicionar credenciais de protocolo e iniciar a detecção

Para detectar seus dispositivos monitorados, conclua as seguintes seções:

## Criar um protocolo ELMC no Insight RS Console

Para configurar o ELMC no Insight RS Console, conclua as seguintes etapas:

1. Em um navegador da Web, faça logon no Insight RS Console.
2. No menu principal, selecione **Detecção** e clique na guia **Credenciais**.
3. Na lista suspensa **Selecionar e configurar protocolo**, selecione **Coletor de monitoramento do log de eventos (ELMC)**.
4. Clique em **Novo**. A caixa de diálogo Nova credencial é exibida.

O Insight RS cria a credencial de protocolo, que é exibida na tabela de credenciais.

# Criar uma credencial de protocolo SNMPv1 no Insight RS Console

Se a cadeia da comunidade SNMPv1 do dispositivo estiver definida como `pública` e o modo de acesso da comunidade for `somente leitura`, o Insight RS associará automaticamente um protocolo SNMP ao seu dispositivo. Se você usar uma cadeia de comunidade diferente ou uma porta não padrão, precisará criar uma credencial de protocolo SNMPv1 no Insight RS Console.

Para configurar o SNMPv1 no Insight RS Console, conclua as seguintes etapas:

1. Em um navegador da Web, faça logon no Insight RS Console.
2. No menu principal, selecione **Detecção** e clique na guia **Credenciais**.
3. Na lista suspensa Selecionar e configurar protocolo, selecione **Simple Network Management Protocol versão 1 (SNMPv1)**.
4. Clique em **Novo**. A caixa de diálogo Nova credencial é exibida.
5. Digite a cadeia de caracteres da comunidade configurada no seu dispositivo.
6. Clique em **Adicionar**.

O Insight RS cria a credencial de protocolo, que é exibida na tabela de credenciais.

# Criar uma credencial de protocolo WMI no Insight RS Console

Para configurar o WMI no Insight RS Console, conclua as seguintes etapas:

1. Em um navegador da Web, faça logon no Insight RS Console.
2. No menu principal, selecione **Detecção** e clique na guia **Credenciais**.
3. Na lista suspensa **Selecionar e configurar protocolo**, selecione **Instrumentação de Gerenciamento do Windows (WMI)**.
4. Clique em **Novo**. A caixa de diálogo Nova credencial é exibida.
5. Digite o nome de usuário e a senha configurados no seu dispositivo.
6. Clique em **Adicionar**.

O Insight RS cria a credencial de protocolo, que é exibida na tabela de credenciais.

# Detectar o dispositivo no Insight RS Console

Para detectar o dispositivo por meio do Insight RS Console, conclua as seguintes etapas:

1. Em um navegador da Web, faça logon no Insight RS Console.
2. No menu principal, selecione **Detecção** e clique na guia **Fontes**.
3. Expanda a seção Endereços IP e adicione o endereço IP do seu dispositivo:
   a. Clique em **Novo**.
   b. Selecione **Endereço único**, **Intervalo de endereços** ou **Lista de endereços**.
   c. Digite os endereços IP dos dispositivos a serem detectados.
   d. Clique em **Adicionar**.
4. Clique em **Iniciar detecção**.

# Verificar o status de detecção e do dispositivo

Para verificar se o dispositivo foi detectado corretamente, conclua as seguintes etapas:

1. Em um navegador da Web, faça logon no Insight RS Console.
2. No menu principal, selecione **Dispositivos** e clique na guia **Resumo do dispositivo**.
3. Verifique se a coluna Status contém um ícone de êxito (✅).

   Se não houver ícone de êxito, tente descobrir que coluna está com problema e consulte a Ajuda on-line para informações de solução de problemas.

# Verificar a comunicação entre o dispositivo monitorado e o Insight RS

Para verificar a comunicação entre o dispositivo monitorado e o Insight RS, conclua as seguintes seções:

# Verificar a conectividade enviando uma interceptação de teste SNMP

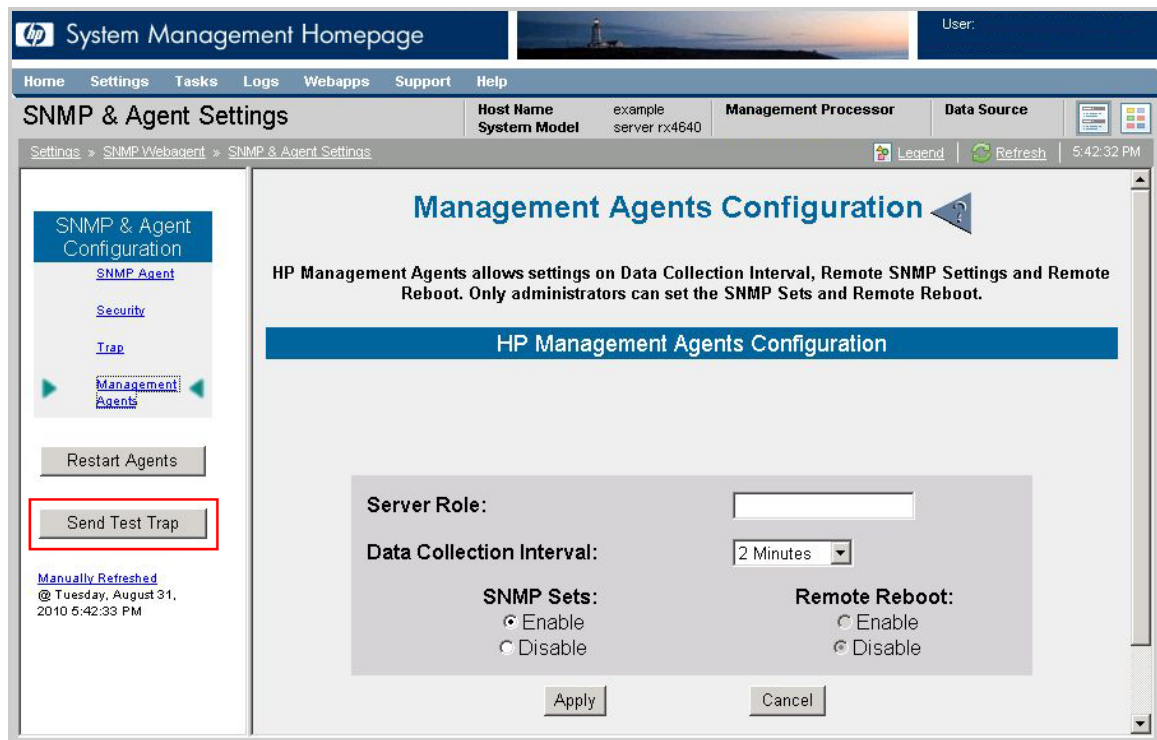
Use agentes SNMP para enviar testes de interceptação de SNMP para verificar a conexão.

1. Em um navegador, acesse o System Management Homepage (SMH) no dispositivo monitorado: `https://[endereçoIP]:2381`.
2. Faça login usando o nome do usuário administrador e a senha do dispositivo monitorado.

**Observação:** Se não aparecer a tela de login, clique no link Entrar no canto superior direito da interface da SMH. Se você não estiver conectado como administrador do dispositivo

monitorado, não terá todas as opções de configuração relevantes.

3. Se o SNMP não estiver definido como sua fonte de dados, clique em **Configurações** na barra de menu superior.
4. Na caixa **Selecionar fonte de dados na SMH**, clique no link **Selecionar**.
5. Na seção Selecionar fonte de dados, escolha a opção **SNMP** e clique em **Selecionar**.

6. Depois que a Fonte de dados estiver configurada como SNMP, clique na opção **Configurações** e selecione **Configuração de SNMP e agente**.
7. Na tela Configuração de agentes de gerenciamento, clique em **Enviar interceptação de teste**.

# Enviar uma indicação de teste de WBEM para verificar a conexão

Use provedores WBEM para enviar indicações de WBEM para verificar a conexão.

1. Em um navegador, acesse o System Management Homepage (SMH) no dispositivo monitorado: `https://[`*`endereçoIP`*`]:2381`.
2. Faça login usando o nome do usuário administrador e a senha do dispositivo monitorado.

**Observação:** Se não aparecer a tela de login, clique no link **Entrar** no canto superior direito da interface da SMH. Você não terá acesso a todas as opções de configuração relevantes se não fizer login como administrador do dispositivo monitorado.

3. Na barra superior do menu, clique em **Configurações**.
4. Se você tiver optado pela instalação de WBEM com o Integrity Support Pack, ele será definido como a sua fonte de dados. Clique na opção **Enviar indicação de teste**.

5. Na tela Enviar indicação de teste, selecione um tipo de ID de evento e clique em **Enviar**.

# Visualizar eventos de teste no Insight RS Console

Alguns tipos de dispositivos monitorados permitem o envio de um evento de teste ao Insight Remote Support. Depois de configurar o dispositivo monitorado e enviar um evento de teste, use o seguinte processo para verificar se o evento de teste chegou.

1. Faça logon no Insight RS Console.
2. No menu principal, selecione **Eventos de serviços**. Se o dispositivo monitorado estiver configurado

adequadamente, o evento aparecerá no painel Informações sobre eventos de serviços.

# Verificar coletas no Insight RS Console

Coletas não são executadas automaticamente depois da descoberta. A HP recomenda que você execute uma coleta manualmente após a descoberta completa para verificar a conectividade. Execute o cronograma de coleta manualmente na guia Serviços de coleta → Agendamentos de coleta. Para obter mais informações sobre o agendamento de coletas, consulte a Ajuda do Insight RS.

Verifique se essa coleta foi bem-sucedida na guia Serviços de coleta → Resultados da coleta básica do Insight RS Console.

1. Faça logon no Insight RS Console.
2. No menu principal, selecione **Serviços de coleta** e depois clique na guia **Resultados da coleta básica**.
3. Expanda a seção Coleta de configurações básicas do servidor.
4. Localize a entrada referente ao seu dispositivo e verifique a coluna Resultado. Se a coleta tiver sido bem-sucedida, um ícone de êxito será exibido (). Se ocorrer uma falha, um ícone de erro será exibido ().

# Capítulo 9: Configurar servidores Integrity Windows 2008

## Atender aos requisitos de configuração

Para configurar servidores Integrity Windows 2008 de forma que eles sejam monitorados pelo Insight RS, conclua as seguintes seções:

**Tabela 9.1** ***Etapas de configuração do servidor Integrity Windows 2008***

| Tarefa | Concluída? |
|---|---|
| Certifique-se de que o Insight RS suporte seu servidor Integrity Windows 2008, verificando o *Notas de Lançamento do HP Insight Remote Support*. | |
| Instale o WBEM no servidor Integrity Windows 2008. | |
| Adicione o protocolo WBEM ao Insight RS Console. | |
| Detecte o servidor Integrity Windows 2008 no Insight RS Console. | |
| Envie um evento de teste para verificar a conectividade entre seu servidor Integrity Windows 2008 e o Insight RS. | |

# Instalar e configurar o software de comunicação em servidores

Para configurar seus dispositivos monitorados, conclua as seguintes seções:

## Instalar provedores WBEM no dispositivo monitorado

Para que o dispositivo monitorado Windows 2008 Integrity seja detectado pelo Insight RS Console e compatível com coletas de configuração, é necessário que o HP Integrity WBEM Providers para Windows Server 2008 está instalado e totalmente configurado nos dispositivos monitorados, conforme as instruções que constam na documentação do produto HP Smart Setup do respectivo pacote. Os dispositivos Integrity Windows 2008 monitorados também usam WBEM para envio de evento/monitoramento remoto.

Os servidores Integrity Windows fabricados pela HP já acompanham os arquivos de instalação Smart Setup pré-carregados no disco do sistema operacional. Nos demais casos, os pacotes podem ser instalados usando o CD Smart Setup ou a mídia de reinstalação. Você pode baixar o CD Smart Setup ou o Integrity Support Pack em:

- Windows Server 2008: http://h20000.www2.hp.com/bizsupport/TechSupport/SoftwareIndex.jsp?lang=en&cc=us&prodNameId=3346453&prodTypeId=15351&prodSeriesId=3346452&swLang=13&taskId=135&swEnvOID=4023
- Windows Server 2008 R2: http://h20000.www2.hp.com/bizsupport/TechSupport/SoftwareIndex.jsp?lang=en&cc=us&prodNameId=3346453&prodTypeId=15351&prodSeriesId=3346452&swLang=13&taskId=135&swEnvOID=4068

Para que os provedores WBEM se comuniquem com o dispositivo host, você precisa fornecer as credenciais WBEM dentro do Insight RS Console quando estiver concluindo a configuração do Insight Remote Support.

## Definir configurações de firewall e porta

Para obter uma lista completa de requisitos de firewall e de porta para dispositivos monitorados, consulte o *Informe de Segurança do HP Insight Remote Support*, em: http://www.hp.com/go/insightremotesupport/docs.

# Adicionar credenciais de protocolo e iniciar a detecção

Para detectar seus dispositivos monitorados, conclua as seguintes seções:

## Criar uma credencial de protocolo WBEM no Insight RS Console

Para configurar o WBEM no Insight RS Console, conclua as seguintes etapas:

1. Em um navegador da Web, faça logon no Insight RS Console.
2. No menu principal, selecione **Detecção** e clique na guia **Credenciais**.
3. Na lista suspensa **Selecionar e configurar protocolo**, selecione **Gerenciamento Corporativo baseado na Web (WBEM)**.
4. Clique em **Novo**. A caixa de diálogo Nova credencial é exibida.
5. Digite o nome de usuário e a senha configurados no seu dispositivo.
6. Clique em **Adicionar**.

O Insight RS cria a credencial de protocolo, que é exibida na tabela de credenciais.

## Detectar o dispositivo no Insight RS Console

Para detectar o dispositivo por meio do Insight RS Console, conclua as seguintes etapas:

1. Em um navegador da Web, faça logon no Insight RS Console.
2. No menu principal, selecione **Detecção** e clique na guia **Fontes**.
3. Expanda a seção Endereços IP e adicione o endereço IP do seu dispositivo:
   a. Clique em **Novo**.
   b. Selecione **Endereço único**, **Intervalo de endereços** ou **Lista de endereços**.
   c. Digite os endereços IP dos dispositivos a serem detectados.
   d. Clique em **Adicionar**.
4. Clique em **Iniciar detecção**.

## Verificar o status de detecção e do dispositivo

Para verificar se o dispositivo foi detectado corretamente, conclua as seguintes etapas:

1. Em um navegador da Web, faça logon no Insight RS Console.
2. No menu principal, selecione **Dispositivos** e clique na guia **Resumo do dispositivo**.
3. Verifique se a coluna Status contém um ícone de êxito (✅).

   Se não houver ícone de êxito, tente descobrir que coluna está com problema e consulte a Ajuda on-line para informações de solução de problemas.

# Verificar a comunicação entre o dispositivo monitorado e o Insight RS

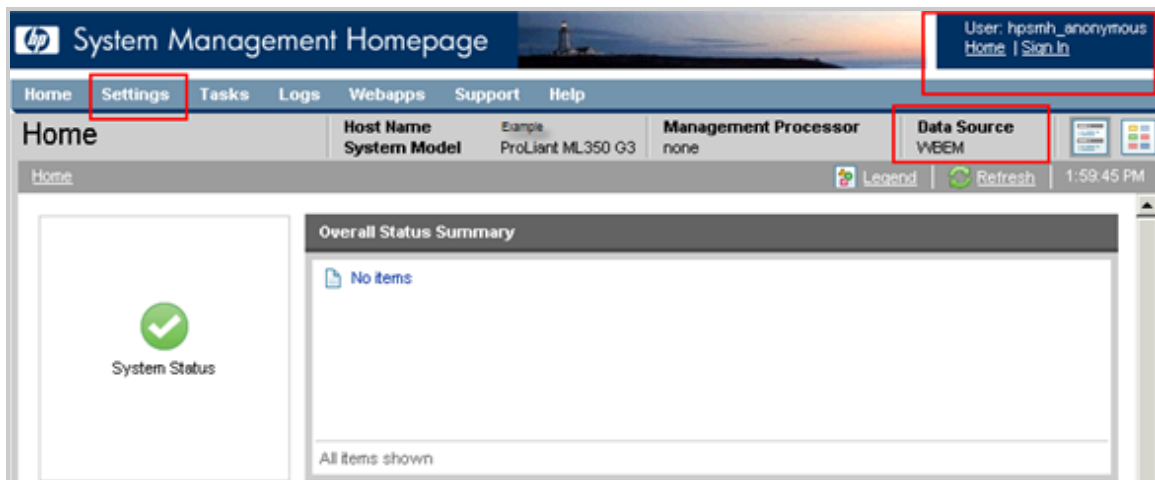
Para verificar a comunicação entre o dispositivo monitorado e o Insight RS, conclua as seguintes seções:

## Verifique a conectividade, enviando uma indicação de teste WBEM

Provedores WBEM podem ser usados para enviar indicações de WBEM para verificar a conexão.

1. Em um navegador, acesse o System Management Homepage (SMH) no dispositivo monitorado: `https://endereçoIP:2381`.
2. Faça login usando o nome do usuário administrador e a senha do dispositivo monitorado.

**Observação:** se não aparecer a tela de login, clique no link **Entrar** no canto superior direito da interface da SMH. Se você não estiver conectado como administrador do dispositivo monitorado, não terá todas as opções de configuração relevantes.

3. Na barra superior do menu, clique em **Configurações**.

4. Se você tiver optado pela instalação de WBEM com o pacote de suporte, ele será definido como sua fonte de dados. Clique na opção **Enviar indicação de teste**.

5. Na tela Enviar indicação de teste, selecione um tipo de ID de evento e clique em **Enviar**.

# Visualizar eventos de teste no Insight RS Console

Alguns tipos de dispositivos monitorados permitem o envio de um evento de teste ao Insight Remote Support. Depois de configurar o dispositivo monitorado e enviar um evento de teste, use o seguinte processo para verificar se o evento de teste chegou.

1. Faça logon no Insight RS Console.
2. No menu principal, selecione **Eventos de serviços**. Se o dispositivo monitorado estiver configurado adequadamente, o evento aparecerá no painel Informações sobre eventos de serviços.

# Verificar coletas no Insight RS Console

Coletas não são executadas automaticamente depois da descoberta. A HP recomenda que você execute uma coleta manualmente após a descoberta completa para verificar a conectividade. Execute o cronograma de coleta manualmente na guia Serviços de coleta → Agendamentos de coleta. Para obter

mais informações sobre o agendamento de coletas, consulte a Ajuda do Insight RS.

Verifique se essa coleta foi bem-sucedida na guia Serviços de coleta → Resultados da coleta básica do Insight RS Console.

1. Faça logon no Insight RS Console.
2. No menu principal, selecione **Serviços de coleta** e depois clique na guia **Resultados da coleta básica**.
3. Expanda a seção Coleta de configurações básicas do servidor.
4. Localize a entrada referente ao seu dispositivo e verifique a coluna Resultado. Se a coleta tiver sido bem-sucedida, um ícone de êxito será exibido (). Se ocorrer uma falha, um ícone de erro será exibido ().

# Capítulo 10: Configurar servidores Integrity Linux

**Importante:** Não há suporte para coletas de configuração.

**Observação:** Não há suporte a nPars em servidores Integrity Linux, exceto em servidores Integrity Superdome X.

## Atender aos requisitos de configuração

Para configurar servidores Integrity Linux de forma que eles sejam monitorados pelo Insight RS, conclua as seguintes seções:

**Tabela 10.1** ***Etapas de configuração do servidor Integrity Linux***

| Tarefa | Concluída? |
|---|---|
| Certifique-se de que o Insight RS suporte seu servidor Integrity Linux, verificando o *Notas de Lançamento do HP Insight Remote Support*. | |
| Verifique se o WBEM está instalado e configurado no servidor Integrity Linux. | |
| Adicione o protocolo WBEM ao Insight RS Console. | |
| Detecte o servidor Integrity Linux no Insight RS Console. | |
| Envie um evento de teste para verificar a conectividade entre seu servidor Integrity Linux e o Insight RS. | |

## Instalar e configurar o software de comunicação em servidores

Para configurar seus dispositivos monitorados, conclua as seguintes seções:

## Verificar os provedores HP WBEM instalados

**Importante:** Ao configurar o Insight Remote Support, você *precisa* configurar as credenciais WBEM para seus dispositivos monitorados Integrity Linux no Insight RS Console. Anote estas credenciais pois será necessário fornecê-las mais tarde.

Os provedores HP WBEM são necessários em seus dispositivos monitorados Integrity Linux. Os provedores HP WBEM Integrity Linux e a documentação relevante são parte do pacote de suporte, que é parte do pacote maior HP Integrity Essentials Foundation for Linux. A HP recomenda a instalação do HP Integrity Essentials Foundation Pack em vez do Agente ou Provedor WBEM do HP Insight Management apenas, pois ele contém atualizações de componentes adicionais recomendadas. Para obter mais detalhes, visite http://h20341.www2.hp.com/integrity/w1/en/os/linux-on-integrity-certification-matrix-novell-suse.html.

Você pode baixar a versão mais recente do software *HP Integrity Essentials Foundation Pack for Linux* em: http://www.hp.com/go/integritylinuxessentials.

## Definir configurações de firewall e porta

Para obter uma lista completa de requisitos de firewall e de porta para dispositivos monitorados, consulte o *Informe de Segurança do HP Insight Remote Support*, em: http://www.hp.com/go/insightremotesupport/docs.

# Adicionar credenciais de protocolo e iniciar a detecção

Para detectar seus dispositivos monitorados, conclua as seguintes seções:

## Criar uma credencial de protocolo WBEM no Insight RS Console

Para configurar o WBEM no Insight RS Console, conclua as seguintes etapas:

1. Em um navegador da Web, faça logon no Insight RS Console.
2. No menu principal, selecione **Detecção** e clique na guia **Credenciais**.
3. Na lista suspensa **Selecionar e configurar protocolo**, selecione **Gerenciamento Corporativo baseado na Web (WBEM)**.
4. Clique em **Novo**. A caixa de diálogo Nova credencial é exibida.
5. Digite o nome de usuário e a senha configurados no seu dispositivo.
6. Clique em **Adicionar**.

O Insight RS cria a credencial de protocolo, que é exibida na tabela de credenciais.

## Detectar o dispositivo no Insight RS Console

Para detectar o dispositivo por meio do Insight RS Console, conclua as seguintes etapas:

1. Em um navegador da Web, faça logon no Insight RS Console.
2. No menu principal, selecione **Detecção** e clique na guia **Fontes**.
3. Expanda a seção Endereços IP e adicione o endereço IP do seu dispositivo:
   a. Clique em **Novo**.
   b. Selecione **Endereço único**, **Intervalo de endereços** ou **Lista de endereços**.
   c. Digite os endereços IP dos dispositivos a serem detectados.
   d. Clique em **Adicionar**.
4. Clique em **Iniciar detecção**.

# Verificar o status de detecção e do dispositivo

Para verificar se o dispositivo foi detectado corretamente, conclua as seguintes etapas:

1. Em um navegador da Web, faça logon no Insight RS Console.
2. No menu principal, selecione **Dispositivos** e clique na guia **Resumo do dispositivo**.
3. Verifique se a coluna Status contém um ícone de êxito (✅).

   Se não houver ícone de êxito, tente descobrir que coluna está com problema e consulte a Ajuda on-line para informações de solução de problemas.

# Verificar a comunicação entre o dispositivo monitorado e o Insight RS

Para verificar a comunicação entre o dispositivo monitorado e o Insight RS, conclua as seguintes seções:

## Enviar um evento de teste para o dispositivo host

Para enviar um evento de teste do dispositivo monitorado para o dispositivo host, digite o seguinte comando na linha de comando do dispositivo monitorado:

```
touch /tmp/SMX.test
```

**Observação:** Esse processo não é compatível com Red Hat Linux 4 ou 5.

Isso cria um arquivo de comprimento zero chamado `SMX.test` no diretório `tmp`. Os provedores SMX criarão uma indicação a ser enviada ao dispositivo host e removerão o arquivo temporário que você criou na etapa anterior.

## Visualizar eventos de teste no Insight RS Console

Alguns tipos de dispositivos monitorados permitem o envio de um evento de teste ao Insight Remote Support. Depois de configurar o dispositivo monitorado e enviar um evento de teste, use o seguinte processo para verificar se o evento de teste chegou.

1. Faça logon no Insight RS Console.
2. No menu principal, selecione **Eventos de serviços**. Se o dispositivo monitorado estiver configurado

adequadamente, o evento aparecerá no painel Informações sobre eventos de serviços.

# Verificar coletas no Insight RS Console

Coletas de configuração não têm suporte para esse tipo de dispositivo, exceto quando ele faz parte de uma coleta de SAN. Se você adicionou esse dispositivo a uma coleta de SAN, poderá executar manualmente uma coleta de SAN para verificar a configuração.

1. Faça logon no Insight RS Console.
2. No menu principal, selecione **Serviços de coleta**.
3. Clique na guia **Agendamentos de coleta**.
4. No painel Lista de agendamentos de coleta, selecione **Agendamento de coletas de configuração da SAN**. Informações sobre a coleta são exibidas no painel Informações da coleta. O painel Nestes dispositivos lista os dispositivos em que a coleta será executada.
5. No painel Informações de agendamento, clique em **Executar agora**.
6. Quando a coleta terminar, clique na guia **Resultados da Coleta de Armazenamento SAN**.
7. Expanda a seção Coleta de Configurações de SAN.
8. Localize a entrada referente ao seu dispositivo e verifique a coluna Resultado. Se a coleta tiver sido bem-sucedida, um ícone de êxito será exibido (). Se ocorrer uma falha, um ícone de erro será exibido ().

# Capítulo 11: Configurar servidores Integrity HP-UX

Antes de tentar configurar o Insight Remote Support para o seu dispositivo monitorado HP-UX, leia as informações a seguir.

**Observação:** O Insight RS 7.4 oferece suporte a vPars v5 do HP-UX 11i v3 nos seguintes servidores Integrity: rx2800 i2, rx2800 i4, BL8x0c i2, BL8x0c i4 e Superdome 2. ***Não*** há suporte para vPars v6.

**Observação:** O Insight Remote Support versão 7.4 apenas oferece suporte para o HP-UX em servidores Integrity.

## Atender aos requisitos de configuração

Para configurar servidores Integrity HP-UX de forma que eles sejam monitorados pelo Insight RS, conclua as seguintes seções:

**Tabela 11.1** ***Etapas de configuração do servidor Integrity HP-UX***

| Tarefa | Concluído? |
|---|---|
| Certifique-se de que o Insight RS suporte seu servidor HP-UX, verificando o *Notas de Lançamento do HP Insight Remote Support*. | |
| Instale os pré-requisitos do Gerenciamento de falhas do sistema, no servidor Integrity HP-UX:<br>• Correções do SO<br>• Protocolo de comunicações de rede segura OpenSSL<br>• Diagnósticos online<br>• Produto principal de serviços WBEM<br>• Web de gerenciamento do sistema | |
| Instale e configure os pré-requisitos do Gerenciamento de falhas do sistema, no servidor Integrity HP-UX. | |
| Configure usuários WBEM no servidor HP-UX. | |
| Defina o firewall para permitir a comunicação em portas específicas. | |
| Adicione o protocolo WBEM ao Insight RS Console. | |
| Detecte o servidor HP-UX no Insight RS Console. | |
| Envie um evento de teste para verificar a conectividade ao dispositivo host. | |

# Instalar e configurar o software de comunicação em servidores

Para configurar seus dispositivos monitorados, conclua as seguintes seções:

# Instalar o Gerenciamento de falhas do sistema

O Gerenciamento de falhas do sistema (SFM) é uma exigência para comunicações do Insight Remote Support em todas as versões com suporte do HP-UX. O SFM tem muitos pré-requisitos de patch, que são detalhados na seção "Atender aos requisitos de sistema operacional, de software e de patch do HP-UX". Se seus sistemas já atendem aos requisitos mínimos identificados nesta seção, você não precisa remover ou reinstalar esses componentes.

**Observação:** Você pode estar familiarizado com os vários provedores SFM disponíveis nas diferentes ofertas SFM. O Insight Remote Support exige apenas os provedores nos pacotes SFM padrão, conforme especificado em "Atender aos requisitos de sistema operacional, software e patch do HP-UX".

O Gerenciamento corporativo baseado na web (WBEM) é uma iniciativa do setor para padronizar informações de gerenciamento em diferentes plataformas. O Gerenciamento de falhas do sistema (SFM) é a solução de gerenciamento de falhas do HP-UX que implementa padrões WBEM. O SFM se integra com outras aplicações de gerenciamento, como o Insight Remote Support e o HP SMH. O SFM requer que o HP-UX tenha os *Serviços WBEM para HP-UX* e outros softwares instalados.

Os eventos em WBEM são chamados de indicações. Antes de uma indicação poder ser comunicada a um sistema cliente (por exemplo, o dispositivo host), o sistema cliente deve assinar o evento. Uma inscrição de evento informa ao *Common Information Model Object Manager* (CIMOM) do dispositivo monitorado que o dispositivo host está interessado em receber indicações daquele dispositivo monitorado. Quando o CIMOM recebe uma indicação de um provedor de indicação, ele envia a indicação para os clientes que já inscreveram para recebê-las.

O Insight Remote Support assina essas indicações. Terminada a assinatura, as indicações são entregues ao Insight Remote Support à medida que elas ocorrem.

Mais informações sobre o SFM e provedores podem ser encontradas em *Informações do depósito OE/AR para provedores WBEM HP-UX*, em: http://h10018.www1.hp.com/wwsolutions/misc/hpsim-helpfiles/OEARInformation.pdf.

Consulte as tabelas a seguir para configurar os dispositivos monitorados HP-UX *antes* de instalar o Insight Remote Support no seu dispositivo host. No dispositivo host, utilize o Insight RS Console para detectar seu dispositivo monitorado e configurar as informações do sistema.

O System Fault Management (SFM) é uma exigência para comunicações do Remote Support em todas as versões com suporte do HP-UX. O SFM tem muitos pré-requisitos de patch que são detalhados nas tabelas a seguir. Se seus sistemas já atendem aos requisitos mínimos, você não precisa remover ou reinstalar estes componentes. Se seus sistemas não atendem aos requisitos mínimos, atualize conforme necessário.

Além disso, você pode estar familiarizado com os vários provedores SFM disponíveis nas diferentes ofertas SFM. O Insight Remote Support requer apenas os provedores nos pacotes SFM padrão especificados nas tabelas abaixo oferece para oferecer suporte aos seus dispositivos monitorados. Uma visão geral desses provedores pode ser vista nas *Informações do depósito OE/AR para provedores WBEM HP-UX*, em: http://h10018.www1.hp.com/wwsolutions/misc/hpsim-helpfiles/OEARInformation.pdf.

**Importante:** No dispositivo host, detecte seu dispositivo monitorado HP-UX e configure as informações do sistema após atender aos pré-requisitos do HP-UX definidos neste capítulo.

# Atender aos requisitos de software e de patch para o HP-UX 11i v2

**Importante:** Embora não seja exigido para o HP-UX 11i v2 (11.23), a HP recomenda instalar o pacote de patch mais recente `QPKBASE`. O `QPKBASE` atende a todos os requisitos de patches do sistema e proporciona um ambiente suportado estável. A tabela abaixo identifica os patches *mínimos* necessários (se o `QPKBASE` não estiver instalado).

**Observação:** *Notas sobre a tabela abaixo*

- Os serviços WBEM, os diagnósticos online e o SysMgmtWeb estão disponíveis na mídia do ambiente operacional (OE) e podem ser selecionados para instalação durante a instalação do SFM.
- As versões de software listadas são os requisitos mínimos suportados. Versões mais recentes são suportadas, salvo se houver indicação contrária.
- A Página Inicial do Gerenciamento de Sistemas (SHM), incluída no SysMgmtWeb, é opcional, mas permite que você use o componente EVWEB GUI do SFM para visualizar eventos manipulados pelo SFM no host.
- A tabela lista os itens na sequência em que devem ser instalados no caso de algum deles estar faltando e de ser necessária a atualização ou instalação.

**Tabela 11.2** ***Componentes de software necessários para o HP-UX 11i v2***

| Software necessário | Versão necessária |
|---|---|
| *Ambiente operacional HP-UX* | • Setembro de 2004, OE 11i v2 (versão OE mínima)<br>• Maio de 2005, OE 11i v2 (necessário para habilitar o vPars). |
| Como baixar ou acessar o software: http://www.hp.com/go/hpux11ioe | |
| | |

**Tabela 11.2** ***Componentes de software necessários para o HP-UX 11i v2, continuação***

<table>
<tr><th>Software necessário</th><th>Versão necessária</th></tr>
<tr><td>Requisitos de correções de sistemas operacionais<br><br>Observação: Estes seis patches adicionais para o HP-UX 11i v2 não fazem parte do Bundle11i e devem ser instalados junto com ele.</td><td>Patch BUNDLE 11i, pacote B.11.23.0409.3 (setembro de 2004):<ul><li>PHKL_36288 - 11.23 driver cumulativo diag2 e habilitação vPars (use em substituição ao PHKL_32653), exige reinicialização</li><li>PHKL_34795 - 11.23 driver patch cumulativo IPMI, exige reinicialização</li><li>PHSS_37552 - 1.0 Patch cumulativo Aries</li><li>PHSS_37947 - 1.0 vinculador + patch cumulativo fdp</li><li>PHSS_35055 - Tempo de execução aC++ (IA: A.06.10, PA: A.03.71)</li><li>PHSS_36345 - 11.23 Integrity Unwind Library</li></ul></td></tr>
<tr><td colspan="2">Como baixar ou acessar o software:<br><br>Acesse http://www.hp.com/go/hpsc e faça logon usando sua conta do HP Passaporte. No menu esquerdo, clique no link Gerenciamento de patches. Digite o nome do patch na caixa de pesquisa Gerenciamento de patch e clique em IR.</td></tr>
<tr><td colspan="2"></td></tr>
<tr><td>Protocolo de comunicações de rede segura OpenSSL</td><td>Pacote de produtos A.00.09.07i.012 (dezembro de 2006) ou posterior</td></tr>
<tr><td colspan="2">Como baixar ou acessar o software:<ul><li>Disponível na mídia do aplicativo, a partir de dezembro de 2006</li><li>Se preferir, acesse o seguinte local do HP Software Depot para obter a versão mais recente: https://h20392.www2.hp.com/portal/swdepot/try.do?productNumber=OPENSSL11I</li></ul></td></tr>
<tr><td colspan="2"></td></tr>
<tr><td>Diagnósticos online</td><td>Pacote de ferramentas de suporte B.11.23.10.05 HPUX 11.23 (dezembro de 2007) ou posterior</td></tr>
<tr><td colspan="2">Como baixar ou acessar o software:<ul><li>Disponível na mídia HWE0706</li><li>Se preferir, acesse o seguinte local do HP Software Depot para obter a versão mais recente: https://h20392.www2.hp.com/portal/swdepot/try.do?productNumber=B6191AAE</li></ul></td></tr>
<tr><td colspan="2"></td></tr>
<tr><td>WBEMSvcs (produto principal de serviços WBEM)</td><td>Produto principal de serviços WBEM A.02.05.08 (dezembro de 2007) ou posterior</td></tr>
<tr><td colspan="2">Como baixar ou acessar o software:<ul><li>Disponível na mídia do aplicativo, a partir de dezembro de 2007</li><li>Se preferir, acesse o seguinte local do HP Software Depot para obter a versão mais recente: https://h20392.www2.hp.com/portal/swdepot/try.do?productNumber=WBEMSvcs</li></ul></td></tr>
<tr><td colspan="2"></td></tr>
</table>

**Tabela 11.2 *Componentes de software necessários para o HP-UX 11i v2, continuação***

| Software necessário | Versão necessária |
|---|---|
| *System Management Web* (recomendado para monitoramento de eventos, necessário para a coleta de configuração) | *Interface de usuário do gerenciamento de sistema baseado na web do HP-UX A.2.2.7 (dezembro de 2007) ou posterior* |
| A Web de gerenciamento de sistema é recomendada para se obter o máximo proveito do componente EVWEB GUI do SFM, que permite a visualização de eventos tratados pelo SFM no host.<br><br>Se apenas a versão 2.2.6.2 do SysMgmtHomepage estiver presente no servidor, a seguinte correção também deverá ser aplicada:<br><br>Para o HP-UX 11i v2 (11.23) OE, aplique o patch **PHSS_36870**<br><br>Os patches podem ser obtidos no Centro de suporte HP:<br><br>Acesse http://www.hp.com/go/hpsc e faça logon usando sua conta do HP Passaporte. No menu esquerdo, clique no link **Gerenciamento de patches**. Digite o nome do patch na caixa de pesquisa Gerenciamento de patch e clique em **IR**<br><br>Isto é um "sharfile" e deve ser descompactado executando-o como um script ("sh PHSS_36870). Observe as instruções de instalação do patch no arquivo de texto incluído (`PHSS_36870.text`) | |
| Como baixar ou acessar o software:<br><br>• Disponível na mídia do software do aplicativo a partir de setembro de 2007<br>• Se preferir, acesse o seguinte local do HP Software Depot para obter a versão mais recente: https://h20392.www2.hp.com/portal/swdepot/try.do?productNumber=SysMgmtWeb | |
| | |
| *System Fault Management (SFM)* | *Gerenciamento de falhas de sistema B.07.01.01.yy (maio de 2009) ou posterior* |
|  **Importante:** É *fundamental* que o SFM seja o último componente de software pré-requisitado a ser instalado ou atualizado a partir desta lista. | |
| Como baixar ou acessar o software:<br><br>• Disponível na mídia HWE0712<br>• Se preferir, acesse o seguinte local do HP Software Depot para obter a versão mais recente: https://h20392.www2.hp.com/portal/swdepot/displayProductInfo.do?productNumber=SysFaultMgmt<br><br> **Observação:** Consulte as *Notas de versão do Gerenciamento de Falhas do Sistema* para mais detalhes e pré-requisitos adicionais do SFM. | |

# Atender aos requisitos de software e de patch para o HP-UX 11i v3

**Observação:** *Notas sobre a tabela abaixo*

- Os serviços WBEM, os diagnósticos online e o SysMgmtWeb estão disponíveis na mídia do ambiente operacional (OE) e podem ser selecionados para instalação durante a instalação do SFM.
- As versões listadas do software são os requisitos mínimos suportados. Versões mais recentes são suportadas, salvo se houver indicação contrária.
- A Página Inicial do Gerenciamento de Sistemas (SHM), incluída no SysMgmtWeb, é opcional, mas permite que você use o componente EVWEB GUI do SFM para visualizar eventos manipulados pelo SFM no host.
- A tabela lista os itens na sequência em que devem ser instalados no caso de algum deles estar faltando e de ser necessária a atualização ou instalação.

**Tabela 11.3** ***Componentes de software necessários para o HP-UX 11i v3***

| Software necessário | Versão necessária |
|---|---|
| *Ambiente operacional HP-UX* | HP-UX 11i v3 |
| Como baixar ou acessar o software: http://www.hp.com/go/hpux11ioe | |
| | |
| *Requisitos de correções de sistemas operacionais* | • EVM-Event Mgr B.11.31<br>• Controlador de Gerenciamento de Placa-base (BMC) versão de firmware 05.21 ou posterior<br>• SysMgmtBase B.00.02.03 ou posterior |
| Como baixar ou acessar o software:<br>Acesse http://www.hp.com e clique na guia Suporte e drivers. Em seguida, clique no botão Baixar patches para o HP-UX, Open VMS, Tru64 e MPE, no lado direito da página. Isso permite o acesso ao ITRC, onde é possível procurar o patch apropriado. | |
| | |
| Protocolo de comunicações de rede segura *OpenSSL* | *A.00.09.07e.013 ou posterior* |
| Como baixar ou acessar o software:<br>• Disponível na mídia do software do aplicativo a partir de setembro de 2007<br>• Se preferir, acesse o seguinte local do HP Software Depot para obter a versão mais recente: https://h20392.www2.hp.com/portal/swdepot/try.do?productNumber=OPENSSL11I | |
| | |
| *Diagnósticos online*: Ferramentas de diagnóstico e suporte para HP-UX, incluindo o STM versão A.49.10 ou posterior e o EMS versão A.04.20 ou posterior | *B.11.31.01.yy ou posterior* (dependência da versão do SysFaultMgmt) |
| Como baixar ou acessar o software:<br>• Disponível na mídia HP-UX 11i v3, de fevereiro de 2007<br>• Se preferir, acesse o seguinte local do HP Software Depot para obter a versão mais recente:<br>https://h20392.www2.hp.com/portal/swdepot/try.do?productNumber=B6191AAE | |
| | |

**Tabela 11.3** ***Componentes de software necessários para o HP-UX 11i v3, continuação***

<table>
<tr><th>Software necessário</th><th>Versão necessária</th></tr>
<tr><td>WBEMSvcs (produto principal de serviços WBEM)</td><td>A.02.05 ou posterior</td></tr>
<tr><td colspan="2">Como baixar ou acessar o software:<br><ul><li>Disponível na mídia do software do aplicativo a partir de setembro de 2007</li><li>Se preferir, acesse o seguinte local do HP Software Depot para obter a versão mais recente: https://h20392.www2.hp.com/portal/swdepot/try.do?productNumber=WBEMSvcs</li></ul></td></tr>
<tr><td colspan="2"></td></tr>
<tr><td>System Management Web (recomendado para monitoramento de eventos, necessário para a coleta de configuração)</td><td>Interfaces de usuário do gerenciamento de sistema baseado na web do HP-UX A.2.2.4 (dezembro de 2007) ou posterior</td></tr>
<tr><td colspan="2">A Web de gerenciamento de sistema é recomendada para se obter o máximo proveito do componente EVWEB GUI do SFM, que permite a visualização de eventos tratados pelo SFM no host.<br><br>Se apenas a versão 2.2.6.2 do SysMgmtHomepage estiver presente no servidor, a seguinte correção também deverá ser aplicada:<br><br>Para o HP-UX 11i v3 (11.31) OE, aplique o patch PHSS_36871<br><br>Os patches podem ser obtidos no Centro de suporte HP:<br><br>Acesse http://www.hp.com/go/hpsc e faça logon usando sua conta do HP Passaporte. No menu esquerdo, clique no link Gerenciamento de patches. Digite o nome do patch na caixa de pesquisa Gerenciamento de patch e clique em IR<br><br>Isto é um "sharfile" e deve ser descompactado executando-o como um script ("sh PHSS_36871). Observe as instruções de instalação do patch no arquivo de texto incluído (<code>PHSS_36871.text</code>)</td></tr>
<tr><td colspan="2">Como baixar ou acessar o software:<br><ul><li>Disponível na mídia do software do aplicativo a partir de setembro de 2007</li><li>Se preferir, acesse o seguinte local do HP Software Depot para obter a versão mais recente: https://h20392.www2.hp.com/portal/swdepot/try.do?productNumber=SysMgmtWeb</li></ul></td></tr>
<tr><td colspan="2"></td></tr>
<tr><td>System Fault Management (SFM)</td><td>Gerenciamento de falhas de sistemas HPUX C.07.10.08.yy ou posteriores</td></tr>
<tr><td colspan="2">É fundamental que o SFM seja o último componente de software pré-requisitado a ser instalado ou atualizado a partir desta lista.</td></tr>
<tr><td colspan="2">Como baixar ou acessar o software:<br><br>A HP recomenda a instalação do SFM através do WBEMMgmtBundle, disponível em:https://h20392.www2.hp.com/portal/swdepot/displayProductInfo.do?productNumber=WBEMMgmtBundle<br><br> Observação: Consulte as Notas de versão do Gerenciamento de Falhas do Sistema para mais detalhes e pré-requisitos adicionais do SFM.</td></tr>
</table>

# Verificar se o Gerenciamento de falhas de sistema está operacional

Para verificar se o componente Gerenciamento de Falhas de Sistema (SFM) está operacional em um dispositivo monitorado HP-UX, siga estas instruções:

1. Execute o seguinte comando para verificar se o componente *HP WBEM Services for HP-UX* está instalado:

   **# swlist | grep -i WBEM**

   O resultado deve ser semelhante ao seguinte:

   ```
   # swlist | grep -i WBEM
     LVMProvider                     R11.23.008      CIM/WBEM Provider for LVM
     ProviderDefault                 B.11.23.0706    Select WBEM Providers
     VMProvider                      A.03.00.76      WBEM Provider for Integrity VM
   ```

2. Para listar os provedores CIM e seus status atuais, a fim de se certificar de que estão todos habilitados, execute o seguinte comando:

   **# cimprovider -l -s**

3. Execute o seguinte comando para verificar se o *OnlineDiag* está instalado e certifique-se de que a versão é a B.11.11.16xx ou posterior:

   **# swlist | grep -i OnlineDiag**

   O resultado deve ser semelhante ao seguinte:

   ```
   # swlist | grep -i OnlineDiag
     OnlineDiag                  B.11.31.03.06   HPUX 11.31 Support Tools Bundle, March 2008
   ```

4. Execute o seguinte comando para verificar se o OnlineDiag está informando que o *Monitoramento de eventos está habilitado atualmente* e que a versão EMS é a A.04.20 ou posterior e a do STM é A.49.10 ou posterior:

   **# /etc/opt/resmon/lbin/monconfig**

   O resultado deve ser semelhante ao seguinte:

```
# /etc/opt/resmon/lbin/monconfig
============================================================================
===================       Event Monitoring Service       ===================
===================      Monitoring Request Manager      ===================
============================================================================

  EVENT MONITORING IS CURRENTLY ENABLED.
  EMS Version : A.04.20.31
  STM Version : D.03.00

============================================================================
==============      Monitoring Request Manager Main Menu      ==============
============================================================================

Note: Monitoring requests let you specify the events for monitors
      to report and the notification methods to use.

Select:
   (S)how monitoring requests configured via monconfig
   (C)heck detailed monitoring status
   (L)ist descriptions of available monitors
   (A)dd a monitoring request
   (D)elete a monitoring request
   (M)odify an existing monitoring request
   (E)nable Monitoring
   (K)ill (disable) monitoring
   (H)elp
   (Q)uit
   Enter selection: [s]
```

5. Selecione '**Q**' para sair do *Menu principal do gerenciador de monitoramento EMS*.
6. Desative os monitores de hardware EMS para o HP-UX 11i v2 e 11i v3.
   a. Verifique se o SFM é usado para monitoramento de hardware:

      **# /opt/sfm/bin/sfmconfig -w -q**

   b. Se o EMS estiver habilitado para o monitoramento, mude para o SFM, usando o comando:

      **# /opt/sfm/bin/sfmconfig -w -s**
7. Execute o seguinte comando para determinar se a versão do componente SMH opcional, mas recomendado, é pelo menos a A.2.2.6.2:

   **# swlist SysMgmtWeb SysMgmtHomepage**

   O resultado deve ser semelhante ao seguinte:

```
# swlist SysMgmtWeb SysMgmtHomepage
# Initializing...
# Contacting target "hpux-server"...
#
# Target:  hpux-server:/
#
# SysMgmtWeb                                A.2.2.8     HP-UX Web Based System Management User Interfaces
# SysMgmtWeb.SysMgmtHomepage                A.2.2.8     HP-UX System Management Homepage - Web-Based User Interfaces
  SysMgmtWeb.SysMgmtHomepage.SMH-DOC        A.2.2.8     HP-UX System Management Homepage Help
  SysMgmtWeb.SysMgmtHomepage.SMH-DOC-COM    A.2.2.8     HP-UX System Management Homepage Help
  SysMgmtWeb.SysMgmtHomepage.SMH-PPAGES     A.2.2.8     HP-UX System Management Homepage Property Pages
  SysMgmtWeb.SysMgmtHomepage.SMH-PPAGES-COM A.2.2.8     HP-UX System Management Homepage Property Pages (common files)
  SysMgmtWeb.SysMgmtHomepage.SMH-RUN        A.2.2.8     HP-UX System Management Homepage Runtime Core
  SysMgmtWeb.SysMgmtHomepage.SMH-SAMLOG     A.2.2.8     HP-UX System Management Homepage LogViewer Web Application
  SysMgmtWeb.SysMgmtHomepage.SMH-UILIB      A.2.2.8     HP-UX System Management Homepage User Interface Library
  SysMgmtWeb.SysMgmtHomepage.SMH-UILIB-COM  A.2.2.8     HP-UX System Management Homepage User Interface Library (common files)
  SysMgmtWeb.SysMgmtHomepage.SMH-XLAUNCH    A.2.2.8     HP-UX System Management Homepage Xlaunch Web Application
```

8. Altere o modo de inicialização para SMH, para que o modo autoiniciar URL seja definido como `OFF` (Desligado) e o modo iniciar com a inicialização seja definido como `ON` (Ligado):

   ```
   # /opt/hpsmh/lbin/hpsmh stop # /opt/hpsmh/bin/smhstartconfig -a off -b on #
   /opt/hpsmh/lbin/hpsmh start # /opt/hpsmh/bin/smhstartconfig
   ```

   ```
   HPSMH 'autostart url' mode.........: OFF HPSMH 'start on boot' mode.........: ON
   Start Tomcat when HPSMH starts.....: OFF
   ```

# Instalar pré-requisitos vPar v5 (se necessário)

Os seguintes arquivos precisam estar instalados no servidor HP-UX 11i v3 para permitir o suporte de vPars v5 com o Insight RS.

- **VirtualPartition A.05,10** – Você precisa do conjunto de arquivos VPAR-RUN desse produto, que faz parte do pacote T1335DC para o recurso vPars v5. O conjunto de arquivos fornece ferramentas de linha de comando de partição virtual que precisam estar disponíveis para que o provedor WBEM VPar funcione corretamente.

  Para verificar se você tem esse pacote instalado, execute o comando **`swlist -l bundle`**. Você verá uma saída semelhante à seguinte:

  ```
  Partições virtuais T1335DC HP-UX para 11.31 A.05.10
  ```

- **VParProvider B.11.31.01.06** – Esse conjunto de arquivos está disponível como parte do Pacote de gerenciamento WBEM, disponível em: https://h20392.www2.hp.com/portal/swdepot/displayInstallInfo.do?productNumber=WBEMMgmtBundle.
- **HP-UX WBEM Services A.02.07** – Esse conjunto de arquivos está disponível como parte do Pacote de gerenciamento WBEM, disponível em: https://h20392.www2.hp.com/portal/swdepot/displayInstallInfo.do?productNumber=WBEMMgmtBundle.

Observe que você já pode ter instalado o Pacote de gerenciamento WBEM quando instalou o SFM.

# Criar usuários do WBEM

O Insight RS requer que usuário e senha dos serviços WBEM, para se comunicar com o dispositivo monitorado HP-UX. Você pode criar um usuário sem privilégios ou, se estiver usando o WBEM A.02.09.08 ou posterior, crie um usuário com privilégios, no arquivo de configuração do Insight Remote.

Se você estiver usando o HP-UX 11i v2 ou v3 e uma versão dos serviços WBEM anterior à A.02.09.08, consulte "Criar usuários sem privilégios com cimauth".

Se você estiver usando o HP-UX 11i v2 ou v3 e os serviços WBEM A.02.09.08 ou posterior, consulte "Criar usuários com privilégios WBEM com o WBEM A.02.09.08 ou posterior".

Para detalhes sobre o SysFaultMgmt, incluindo como definir contas de usuário/senha no WBEM, consulte o *Guia de administração do Gerenciamento de Falhas de Sistema HP-UX*, em: http://www.hp.com/go/hpux-diagnostics-sfm-docs.

## Criar usuários sem privilégios com cimauth

É possível usar uma conta sem privilégios para a comunicação WBEM. Crie ou use um usuário sem privilégios existente. O nome de usuário especificado deve representar um usuário do HP-UX válido no host local.

Para configurar uma conta sem privilégios em um dispositivo monitorado HP-UX, siga estas instruções:

1. Crie um usuário, *hpirs* neste exemplo, e atribua o usuário ao grupo *users*:

   **# useradd –g users hpirs**

2. Defina a senha para o usuário *hpirs*:

   **#passwd hpirs** (quando solicitado, forneça e confirme a senha)

3. Analise a configuração CIM atual, conforme abaixo:

   **# cimconfig –l –p**

   *Exemplo de resultado:*

   ```
   sslClientVerificationMode=disabled
   enableSubscriptionsForNonprivilegedUsers=false
   shutdownTimeout=30
   authorizedUserGroups=
   enableRemotePrivilegedUserAccess=false
   enableHttpsConnection=true
   enableHttpConnection=false
   ```

4. Baseado no resultado acima, defina as seguintes variáveis na configuração planejada CIM:

   **# cimconfig –s enableSubscriptionsForNonprivilegedUsers=true –p**

   **# cimconfig –s enableNamespaceAuthorization=true –p**

5. Parar e iniciar o servidor CIM para definir as alterações de configuração na configuração CIM atual:

   **# cimserver –s**

   **# cimserver**

6. Verificar as configurações na configuração CIM atual:

   **# cimconfig –l -c**

   *Exemplo de resultado:*

   ```
   sslClientVerificationMode=disabled
   enableSubscriptionsForNonprivilegedUsers=true
   shutdownTimeout=30
   authorizedUserGroups=
   ```

```
enableRemoteprivilegedUserAccess=true
enableHttpsConnection=true
enableNamespaceAuthroization=true
enableHttpConnection=false
```

7. Adicionar permissões de leitura e escrita para o usuário *hpirs* a cada um dos namespaces, root/cimv2, root/PG_InterOp e root/PG_Internal:

   **# cimauth –a –u *hpirs* –n root/cimv2 –R –W**

   **# cimauth –a –u *hpirs* –n root/PG_InterOp –R –W**

   **# cimauth –a –u *hpirs* –n root/PG_Internal –R –W**

   **# cimauth –a –u *hpirs* –n root/cimv2/npar –R –W**

   **# cimauth –a –u *hpirs* –n root/cimv2/vpar –R –W**

8. Verificar as permissões do usuário:

   **#cimauth -l**

   *Exemplo de resultado:*

   ```
   hpirs, root/PG_InterOp, "rw"
   hpirs, root/PG_Internal, "rw"
   hpirs, root/cimv2, "rw"
   ```

## *Criar usuários com privilégios WBEM com o WBEM A.02.09.08 ou posterior*

O modo de se especificarem usuários com privilégios no WBEM versão A.02.09.08 para servidores HP-UX 11iv2 e 11iv3 mudou, e não é mais necessário usar comandos `cimauth`. Os serviços HP WBEM versão A.02.09.08 e posteriores suporta a configuração do Insight Remote Support nos sistemas operacionais HP-UX 11i v2 e HP-UX 11i v3.

Após se instalar o WBEM versão A.02.09.08 em servidores HP-UX 11iv2 e 11iV3 anteriormente funcionais monitorados pelo Insight Remote Support, a funcionalidade de monitoramento pode deixar de funcionar. Isso se deve principalmente a como os usuários privilegiados são especificados. Nas versões anteriores, o root era o usuário padrão, e os usuários adicionais com privilégios de root tinham que ser adicionados e configurados com o comando `cimauth` no servidor HP-UX. Com o WBEM versão A.02.09.08 e superiores, isso é feito com um arquivo de configuração do Insight Remote Support, que contém um usuário padrão chamado `hp_irs`.

Essa atualização remove a necessidade de se fornecerem credenciais de root para acesso WBEM ou de se criarem usuários especiais com privilégios root e sem acesso ao sistema, para serem usados com o WBEM.

Para configurar os privilégios de root para usuários do Insight Remote Support em um sistema HP-UX, siga estas instruções:

1. Instale os serviços HP WBEM versão A.02.09.08 ou posterior, nos sistemas operacionais HP-UX 11i v3 e 11i v2.

2. No servidor HP-UX, edite o arquivo de configuração do Insight Remote Support localizado em: `/var/opt/wbem/hp_irs_users.conf` e digite o nome de usuário requerido. Por padrão, o nome de usuário `hp_irs` é adicionado ao arquivo de configuração do Insight Remote Support.

   **Observação:** Somente administradores do sistema podem modificar ou criar nomes de usuários no arquivo de configuração do Insight Remote Support. Assegure-se de que o nome de usuário exista no sistema HP-UX, antes de configurá-lo no arquivo de configuração do Insight Remote Support.

3. Altere `enableSubscriptionsForNonprivilegedUsers` para true:

   **`# cimconfig -s enableSubscriptionsForNonprivilegedUsers=true -p`**

4. Interrompa os serviços WBEM:

   **`# cimserver -s`**

5. Reinicie os serviços WBEM:

   **`# cimserver`**

**Observação:** Os usuários configurados no arquivo de configuração do Insight Remote Support podem executar operações WBEM com privilégios de root. Entretanto, esses usuários ainda podem continuar a ter privilégios do sistema, conforme definidos no arquivo `/etc/passwd` do HP-UX.

**Importante:** Para versões anteriores do WBEM e as que tenham usuários configurados com o comando `cimauth`, os serviços WBEM podem parar de funcionar, após se executar o comando `update-ux` (atualizar para a versão de setembro de 2011 do HP-UX). O pacote WBEM está em um estado *Installed* (Instalado), quando deveria estar em um estado *Configured* (Configurado). Execute `swconfig` em todos os filesets, para resolver esse problema.

Assim que o WBEM versão A.02.09.09 estiver instalado, atualize as credenciais/protocolos do WBEM no Insight RS ou no HP SIM para refletir o novo usuário `hp_irs` ou adicione os usuários anteriormente criados ao arquivo `hp_irs_users.conf`.

Para mais informações sobre o WBEM, consulte o *Guia dos serviços HP WBEM para o administrador do sistema HP-UX*.

# Definir configurações de firewall e porta

Para obter uma lista completa de requisitos de firewall e de porta para dispositivos monitorados, consulte o *Informe de Segurança do HP Insight Remote Support*, em: http://www.hp.com/go/insightremotesupport/docs.

# Adicionar credenciais de protocolo e iniciar a detecção

Para detectar seus dispositivos monitorados, conclua as seguintes seções:

# Adicionar o protocolo WBEM ao Insight RS Console

O Insight RS associa automaticamente o protocolo WBEM configurado no Insight RS Console com o servidor HP-UX.

## Opção 1: Autenticar usando o nome de usuário e a senha

Para configurar o WBEM no Insight RS Console, conclua as seguintes etapas:

1. Em um navegador da Web, faça logon no Insight RS Console.
2. No menu principal, selecione **Detecção** e clique na guia **Credenciais**.
3. Na lista suspensa **Selecionar e configurar protocolo**, selecione **Gerenciamento Corporativo baseado na Web (WBEM)**.
4. Clique em **Novo**. A caixa de diálogo Nova credencial é exibida.
5. Digite o nome de usuário e a senha configurados no seu dispositivo. Use o usuário que foi criado anteriormente em "Criar usuários do WBEM", na página 1.
6. Clique em **Adicionar**.

O Insight RS cria a credencial de protocolo, que é exibida na tabela de credenciais.

## Opção 2: Autenticar no HP-UX WBEM usando um certificado

**Importante:** Repita estas instruções uma vez por ano. O certificado Jetty é válido por um ano, e, enquanto ele se renova automaticamente todo ano, ele precisa ser movido para o servidor HP-UX, após ele se renovar. Para ver quando o certificado Jetty expira, altere a extensão do arquivo de `.pem` para `.cer` e abra o certificado, para ver os detalhes de propriedade.

Para copiar o certificado para o servidor HP-UX, siga estas instruções:

1. No dispositivo host, abra uma janela do DOS e exporte o certificado público para um arquivo chamado `UCACMS.pem`, de modo que ele possa ser movido para o servidor HP-UX:

   ```
   rsadmin cert -export -out c:\temp\UCACMS.pem
   ```

2. Envie, por FTP, o arquivo `UCACMS.pem` no formato ASCII para a pasta `cimserver_trust`, no servidor HP-UX:

   ```
   # ftp <endereço_ip_servidor_hp-ux>
   ftp> cd /etc/opt/hp/sslshare/cimserver_trust/
   ftp> ASCII
   ftp> put UCACMS.pem
   ftp> quit
   ```

3. No dispositivo host, faça logon remotamente no servidor HP-UX.
4. Navegue até o seguinte diretório:

```
cd /etc/opt/hp/sslshare/cimserver_trust/
```

5. Digite os comandos a seguir para configurar a autenticação do certificado WBEM no servidor HP-UX:
   a. Associe o certificado `UCACMS.pem` do Insight RS ao usuário root:

      **`# cimtrust -a -U root -f /etc/opt/hp/sslshare/cimserver_trust/UCACMS.pem -T s`**

   b. Associe o certificado HP-UX ao usuário root:

      **`# cimtrust -a -U root -f /etc/opt/hp/sslshare/cert.pem -T s`**

   c. Verifique os valores atuais de `cimom`:

      ```
      # cimconfig -l -c
      enableAuditLog=false
      sslClientVerificationMode=optional
      idleConnectionTimeout=0
      enableSubscriptionsForNonprivilegedUsers=true
      socketWriteTimeout=20
      shutdownTimeout=30
      authorizedUserGroups=
      enableRemotePrivilegedUserAccess=true
      enableHttpsConnection=true
      enableNamespaceAuthorization=true
      enableHttpConnection=false
      ```

   d. Certifique-se de que os campos em vermelho estejam definidos como acima. Se não estiverem, altere os valores e os valide usando os seguintes comandos:
      i. Defina `sslClientVerificationMode` para `optional`:

         **`# cimconfig -s sslClientVerificationMode=optional -p`**

      ii. Defina `enableHttpsConnection` para `true`:

         **`# cimconfig -s enableHttpsConnection=true -p`**

      iii. Interrompa o daemon `cimom`:

         **`# cimserver -s`**

      iv. Inicie o daemon `cimom`:

         **`# cimserver`**

6. No Insight RS Console, adicione uma credencial de certificado WBEM na guia **Detecção → Credenciais**.
   a. Na lista suspensa **Selecionar e configurar protocolo**, selecione **Gerenciamento Corporativo baseado na Web (WBEM)**.
   b. Clique em **Novo**. A caixa de diálogo Nova credencial é exibida.
   c. Selecione **Credencial de certificado** na lista suspensa **Tipo**.

d. Deixe o campo **Carregar arquivo** em branco, porque o certificado já está no repositório de certificados e é identificado usando-se o nome de alias.

e. Digite um alias de certificado igual a “jetty”, que foi o alias dado ao certificado quando ele foi exportado acima.

# Detectar o dispositivo no Insight RS Console

Para detectar o dispositivo por meio do Insight RS Console, conclua as seguintes etapas:

1. Em um navegador da Web, faça logon no Insight RS Console.
2. No menu principal, selecione **Detecção** e clique na guia **Fontes**.
3. Expanda a seção Endereços IP e adicione o endereço IP do seu dispositivo:
   a. Clique em **Novo**.
   b. Selecione **Endereço único**, **Intervalo de endereços** ou **Lista de endereços**.
   c. Digite os endereços IP dos dispositivos a serem detectados.
   d. Clique em **Adicionar**.
4. Clique em **Iniciar detecção**.

# Verificar o status de detecção e do dispositivo

Para verificar se o dispositivo foi detectado corretamente, conclua as seguintes etapas:

1. Em um navegador da Web, faça logon no Insight RS Console.
2. No menu principal, selecione **Dispositivos** e clique na guia **Resumo do dispositivo**.
3. Verifique se a coluna Status contém um ícone de êxito ().

   Se não houver ícone de êxito, tente descobrir que coluna está com problema e consulte a Ajuda on-line para informações de solução de problemas.

# Verificar a comunicação entre o dispositivo monitorado e o Insight RS

Para verificar a comunicação entre o dispositivo monitorado e o Insight RS, conclua as seguintes seções:

## Verificar a conectividade enviando um teste de interceptação SNMP ao dispositivo host

Envie um evento de teste do servidor HP-UX para verificar a comunicação entre o servidor HP-UX e o dispositivo host. Execute um dos seguintes comandos no servidor HP-UX:

```
# /etc/opt/resmon/lbin/send_test_event disk_em
```

ou

```
# /opt/sfm/bin/sfmconfig -t -a
```

Para detalhes sobre o SysFaultMgmt, incluindo emitir eventos de teste, consulte o *Guia de administração do Gerenciamento de Falhas do Sistema HP-UX*, em: http://www.hp.com/go/hpux-diagnostics-sfm-docs.

## Verificar coletas no Insight RS Console

Coletas não são executadas automaticamente depois da descoberta. A HP recomenda que você execute uma coleta manualmente após a descoberta completa para verificar a conectividade. Execute o cronograma de coleta manualmente na guia Serviços de coleta → Agendamentos de coleta. Para obter mais informações sobre o agendamento de coletas, consulte a Ajuda do Insight RS.

Verifique se essa coleta foi bem-sucedida na guia Serviços de coleta → Resultados da coleta básica do Insight RS Console.

1. Faça logon no Insight RS Console.
2. No menu principal, selecione **Serviços de coleta** e depois clique na guia **Resultados da coleta básica**.
3. Expanda a seção Coleta de configurações básicas do servidor.
4. Localize a entrada referente ao seu dispositivo e verifique a coluna Resultado. Se a coleta tiver sido bem-sucedida, um ícone de êxito será exibido (). Se ocorrer uma falha, um ícone de erro será exibido ().

# Capítulo 12: Configurar servidores Integrity Superdome 2

O complexo do sistema Superdome 2 tem duas interfaces independente que relata indicações de evento: as partições do HP-UX e o Administrador incorporado Superdome 2 (OA). O Gerenciador de falhas do sistema HP-UX (SFM) monitora os dispositivos de ES dentro do domínio da partição e gera indicações WBEM quando ele determina que um evento importante ocorreu. O OA monitora o restante do hardware do sistema e gera indicações WS-Management quando ele determina que ocorreu um evento importante. Para habilitar o monitoramento do sistema completo, tanto o OA quanto as partições devem ser monitorados.

O Insight RS requer o WS-Man para monitorar o OA do Integrity Superdome 2. Se for necessário enviar interceptações SNMP a outro aplicativo de gerenciamento corporativo, lembre-se de não enviar essas interceptações ao mesmo dispositivo host no qual o Insight RS está instalado. Se os dispositivos hosts receberem interceptações SNMP além das notificações necessárias para o WS-Man, as notificações duplicadas serão enviadas à HP.

**Observação:** O Insight RS oferece suporte para vPars v5 do HP-UX 11i v3 em servidores Integrity Superdome 2. ***Não*** há suporte para vPars v6 . Para conhecer os pré-requisitos necessários, consulte Configurar servidores Integrity HP-UX.

**Importante:** Se você atualizou a partir do Insight RS 7.0.5, os servidores Superdome 2 não tinham suporte na versão 7.0.5. Se você detectou seus servidores Superdome 2 na versão 7.0.5, eles apareceram como dispositivos desconhecidos no Insight RS Console. Depois de atualizar para a versão 7.4, eles aparecerão corretamente como servidores Superdome 2, mas o Insight RS não poderá monitorá-los até que você conclua as etapas abaixo e redescubra o servidor Superdome 2.

## Atender aos requisitos de configuração

Para configurar servidores Integrity Superdome 2 de forma que eles sejam monitorados pelo Insight RS, conclua as seguintes seções:

**Tabela 12.1** ***Etapas de configuração do servidor Integrity Superdome 2***

| Tarefa | Concluído? |
|---|---|
| Certifique-se de que o Insight RS oferece suporte ao seu servidor Integrity Superdome 2, verificando a *Notas de Lançamento do HP Insight Remote Support*. | |
| Verifique as configurações de rede e status de protocolo do Superdome 2. | |
| Adicione o protocolo WBEM ao Insight RS Console. | |
| Adicione o protocolo WS-Man ao Insight RS Console. | |
| Detecte o servidor Superdome 2 no Insight RS Console. | |
| Verifique o Superdome 2 e se as partições foram detectadas corretamente. | |
| Envie um evento de teste para verificar a conectividade ao dispositivo host. | |

# Instalar e configurar o software de comunicação em servidores

Para configurar seus dispositivos monitorados, conclua as seguintes seções:

## Verificação da configuração do Superdome 2 OA

Conecte-se ao Superdome 2 OA usando Telnet, SSH ou um navegador da web (HTTPS) e verifique as configurações de rede e o status do protocolo do OA.

Verifique se as configurações de rede estão corretas, incluindo os endereços de servidor DNS tanto para os OAs ativos e em espera, e verifique se o status do protocolo indica que o WS-Man está habilitado. O WS-Man é o protocolo de relatório de eventos com suporte para o Superdome 2 OA. O SNMP deve estar desabilitado, a não ser que o seu uso seja necessário, pois os agentes SNMP enviam notificações de eventos redundantes ao Insight RS. A HP recomenda que o modo IP do gabinete esteja habilitado.

### *Usar Telnet ou SSH*

1. Faça uma conexão Telnet ou SSH para o Administrador incorporado CLI.
2. Verifique se o DNS está configurado: digite o comando **show network** para mostrar as configurações de rede e o status de protocolo do OA.

### *Usar um navegador da Web*

1. Em um navegador da web, faça login na interface da Web do administrador incorporado.
2. No menu da esquerda, selecione **Informações do gabinete** → **Configurações do gabinete** → **Configurações do gabinete TCP/IP**.
3. Selecione **Acesso de rede** e verifique se WS-Management está habilitado.
4. No menu da esquerda, clique no link **Informações do complexo**, em Visão geral do complexo. Clique na guia **Informações**, para mostrar o número de produto e o número de série.

## Definir configurações de firewall e porta

Para obter uma lista completa de requisitos de firewall e de porta para dispositivos monitorados, consulte o *Informe de Segurança do HP Insight Remote Support*, em: http://www.hp.com/go/insightremotesupport/docs.

# Adicionar credenciais de protocolo e iniciar a detecção

Você deve adicionar as credenciais de protocolo WBEM e WS-Man ao Insight RS Console para que o Insight RS possa se comunicar com o servidor Superdome 2.

Para detectar seus dispositivos monitorados, conclua as seguintes seções:

# Criar uma credencial de protocolo WBEM no Insight RS Console

Para configurar o WBEM no Insight RS Console, conclua as seguintes etapas:

1. Em um navegador da Web, faça logon no Insight RS Console.
2. No menu principal, selecione **Detecção** e clique na guia **Credenciais**.
3. Selecione estes filtros:
   a. Na lista suspensa **Selecionar tipo**, selecione **Servidor**.
   b. Na lista suspensa **Selecionar subtipo**, selecione **HP Integrity HPUX**.
   c. Na lista suspensa **Selecionar e configurar protocolo**, selecione **Gerenciamento Corporativo baseado na Web (WBEM)**.
4. Clique em **Novo**. A caixa de diálogo Nova credencial é exibida.
5. Digite o nome de usuário e a senha configurados nas suas partições. Essas são as credenciais que o Insight RS usará para se comunicar com as partições HP-UX.
6. Clique em **Adicionar**.

# Criar uma credencial de protocolo WS-Man no Insight RS Console

Para configurar o WS-Man no Insight RS Console, conclua as seguintes etapas:

1. Em um navegador da Web, faça logon no Insight RS Console.
2. No menu principal, selecione **Detecção** e clique na guia **Credenciais**.
3. Na lista suspensa **Selecionar e configurar protocolo**, selecione **Protocolo de gerenciamento de serviços da Web (WSMAN)**.
4. Clique em **Novo**. A caixa de diálogo Nova credencial é exibida.
5. Digite o nome de usuário e a senha configurados no OA. Essas são as credenciais que o Insight RS usará para se comunicar com o OA.
6. Clique em **Adicionar**.

# Detectar o servidor Superdome 2 no Insight RS Console

Para detectar o servidor Superdome 2 por meio do Insight RS Console, conclua as seguintes etapas:

1. Em um navegador da Web, faça logon no Insight RS Console.
2. No menu principal, selecione **Detecção** e clique na guia **Fontes**.
3. Expanda a seção Endereços IP e adicione o endereço IP do seu dispositivo:

a. Clique em **Novo**.

b. Selecione **Endereço único**, **Intervalo de endereços** ou **Lista de endereços**.

c. Digite os endereços IP dos OAs e partições HP-UX a serem detectados.

d. Clique em **Adicionar**.

4. Clique em **Iniciar detecção**.

**Observação:** Se a detecção estiver configurada para detectar OAs em espera, ela preencherá a tela de Dispositivos com o mínimo de informações sobre esses dispositivos, pois, apesar de suas interfaces de rede poderem estar ativas e acessíveis, eles não estão monitorando a porta 443 usada para comunicações e, assim, não podem oferecer ao Insight RS informações sobre si mesmos. Da mesma forma, por serem dispositivos em espera, o Insight RS não poderá estabelecer assinaturas de monitoramento diretamente com eles. Se ocorrer um failover do OA, o OA passará a assinatura para o novo Monarch, e o Insight RS continuará a monitorar o OA para verificar se há indicações de eventos usando essa assinatura ativa.

# Verificar a detecção do Superdome 2

Depois de concluída a detecção, selecione **Dispositivos** no menu principal. Verifique se todos os Superdome 2 OAs e todas as partições HP-UX previamente configurados para detecção foram detectados e se o status desses dispositivos mostra o ícone de êxito (✔).

## *Verificar partições HP-UX*

Para dispositivos HP-UX, verifique se as informações de dispositivo estão detalhadas na seção do servidor HP-UX. Consulte "Configurar servidores Integrity HP-UX".

## *Verificar o Superdome 2 OA*

Para verificar as informações de dispositivos Superdome 2 OA, siga estas instruções:

1. No Menu principal, selecione **Dispositivos**. Localize o Superdome 2 OA e clique no seu nome de dispositivo.
2. Na guia **Dispositivo**, expanda a seção Status e verifique se o status do registro é **Registrado** e se Habilitado tem a opção **Sim** selecionada.
3. Expanda a seção Hardware e verifique se Nome de dispositivo, Categoria, Produto, Fornecedor, Endereço IP, Número de série adquirido e Número de produto adquirido estão preenchidos corretamente para o dispositivo.
4. Expanda a seção Garantia e contrato e verifique se os valores listados estão corretos.

**Observação:** Os campos Nome do SO e Versão do SO devem estar em branco, se visualizados a partir da seção Sistema operacional.

5. Expanda a seção Entrega e verifique se as informações estão corretas.
6. Clique em **Salvar alterações**, para concluir o processo de detecção do dispositivo.

**Observação:** O Insight RS apenas monitora o OA Monarch (Ativo). O Insight RS assina o OA que está ativo na ocasião da detecção do Insight RS e usa a assinatura para monitorar eventos. Se ocorrer um failover do OA, o Insight RS continuará a monitorar a assinatura ativa assim que ela for passada pelo OA ativo para o OA em espera. O Insight RS Console continuará a mostrar que está monitorando ativamente o OA ativo configurado previamente (mesmo que esse OA tenha falhado).

**Observação:** Uma configuração do Superdome 2 32s consiste em dois gabinetes unidos em um complexo de servidor único. Cada gabinete tem um OA principal e um em espera que gerencia e monitora esse gabinete. Somente um dos dois OAs ativos no complexo Superdome 2 32s é o OA Monarch do complexo, e ele gera as indicações de evento WS-Man produzidas pelo Mecanismo de análise de erro. Assim como no caso de configurações complexas do Superdome 2 16s, o Insight RS apenas assinará o OA Monarch complexo para indicações de eventos WS-Man e apenas exibirá o OA Monarch em sua página de Entidades gerenciadas.

# Verificar a comunicação entre o dispositivo monitorado e o Insight RS

Para verificar a comunicação entre o dispositivo monitorado e o Insight RS, conclua as seguintes seções:

## Gerar eventos de teste

A versão 2.2.27 do firmware do Superdome 2 ou posteriores suportam a capacidade de um administrador se conectar ao OA e gerar uma indicação de teste WS-Man. Use o procedimento a seguir para gerar uma indicação de teste WS-Man:

1. Faça uma conexão Telnet ou SSH à interface CLI do OA e faça o logon usando uma conta de usuário com privilégios de administrador.
2. Digite o comando **test wsman**.
3. Em um navegador da Web, faça logon no Insight RS Console.
4. No menu principal, selecione **Eventos de serviços**. Clique duas vezes no cabeçalho da coluna Data, para que o evento mais recente apareça no topo, e verifique se o Insight RS recebeu o evento de teste.

"Configurar servidores Integrity HP-UX" descreve como gerar eventos de teste de cada uma das partições HP-UX. Gere um evento de teste e verifique se os eventos de teste SFM do HP-UX foram recebidos e processados pelo Insight RS.

# Verificar coletas no Insight RS Console

Coletas não são executadas automaticamente depois da descoberta. A HP recomenda que você execute uma coleta manualmente após a descoberta completa para verificar a conectividade. Execute o cronograma de coleta manualmente na guia Serviços de coleta → Agendamentos de coleta. Para obter mais informações sobre o agendamento de coletas, consulte a Ajuda do Insight RS.

Verifique se essa coleta foi bem-sucedida na guia Serviços de coleta → Resultados da coleta básica do Insight RS Console.

1. Faça logon no Insight RS Console.
2. No menu principal, selecione **Serviços de coleta** e depois clique na guia **Resultados da coleta básica**.
3. Expanda a seção Coleta de configurações básicas do servidor.
4. Localize a entrada referente ao seu dispositivo e verifique a coluna Resultado. Se a coleta tiver sido bem-sucedida, um ícone de êxito será exibido ( ). Se ocorrer uma falha, um ícone de erro será exibido ( ).

# Capítulo 13: Configurar servidores Integrity Superdome X

O sistema Integrity Superdome X implementou a geração de relatórios para eventos de origem única, fazendo com que todas as indicações de eventos sejam informadas por meio do Onboard Administrator (OA) do Integrity Superdome X. O OA monitora o hardware do sistema central e gera indicações de alertas WS-Management quando determina que um evento importante ocorreu. Os provedores WS-Man para Linux e os provedores Windows WinRM monitoram dispositivos de E/S de partições e também comunicam seus eventos via OA.

Embora o OA seja a única fonte de relatórios de eventos para o sistema inteiro, o Insight RS ainda precisa descobrir as partições para dar suporte a coletas de configuração.

Insight RS requer o WS-Man para monitorar o OA do Integrity Superdome X. Se for necessário enviar interceptações SNMP a outro aplicativo de gerenciamento corporativo, lembre-se de não enviar essas interceptações ao mesmo dispositivo host no qual o Insight RS está instalado. Se os dispositivos hosts receberem interceptações SNMP além das notificações necessárias para o WS-Man, as notificações duplicadas serão enviadas à HP.

## Atender aos requisitos de configuração

Para configurar servidores Integrity Superdome X de forma que eles sejam monitorados pelo Insight RS, conclua as seguintes seções:

**Tabela 13.1** ***Etapas de configuração do servidor Integrity Superdome X***

| Tarefa | Concluído? |
| --- | --- |
| Verifique as configurações de rede e o status de protocolo do Integrity Superdome X. | |
| Adicione credenciais do protocolo WS-Man para o OA e as partições no Insight RS Console. O WS-Man usa a porta 443 para o OA e a porta 5986 para as partições Linux e Windows. | |
| Detecte o servidor Integrity Superdome X no Insight RS Console. | |
| Detecte as partições no Insight RS Console. | |
| Verifique se o OA do Integrity Superdome X e as partições foram detectadas corretamente. | |
| Envie um evento de teste do OA e de partições para verificar a conectividade com o dispositivo host. Verifique se uma coleta foi reunida com êxito do OA e de todas as partições. | |

## Configurar o software de comunicação em servidores

Para configurar seus dispositivos monitorados, conclua as seguintes seções:

## Configurar o OA

Para configurar o OA, conclua as seguintes seções:

## Verificação da configuração do OA do Integrity Superdome X

Conecte-se ao OA do Integrity Superdome X usando Telnet, SSH ou um navegador da Web (HTTPS), conforme detalhado a seguir. Ambas as credenciais de nome de usuário e senha para logon fazem distinção entre maiúsculas e minúsculas.

Verifique se as configurações de rede estão corretas, incluindo os endereços de servidor DNS tanto para os OAs ativos e em espera, e verifique se o status do protocolo indica que o WS-Man está habilitado.

A HP recomenda que o modo IP do gabinete esteja habilitado, pois ele oferece suporte à transmissão do endereço IP do OA ativo para o OA em espera caso ocorra um failover do OA. Se o modo IP do gabinete estiver desabilitado, o IRS deverá ser configurado para descobrir tanto o OA ativo quanto o OA em espera.

A HP recomenda consultar no site www.hp.com para ter certeza de que o OA usa a versão de firmware mais recente.

### Usar Telnet ou SSH

1. Faça uma conexão Telnet ou SSH para o Administrador incorporado CLI.
2. Verifique se o DNS está configurado: digite o comando **show network** para mostrar as configurações de rede e o status de protocolo do OA.

### Usar um navegador da Web

1. Em um navegador da web, faça login na interface da Web do administrador incorporado. É possível usar HTTP ou HTTPS para abrir a conexão com a porta padrão.
2. No menu da esquerda, selecione **Informações do gabinete** → **Configurações do gabinete** → **Configurações do gabinete TCP/IP**.

## Adicionar um usuário em nível de operador (se necessário)

Se não quiser fornecer acesso de administrador ao Superdome X OA, use uma conta de Operador no OA para acesso do Insight RS. Para criar uma conta de Operador, siga as seguintes etapas:

```
Shell > add user <nome>
Shell > set user access <nome> OPERATOR
Shell > assign OA <nome>
Shell > assign partition all <nome>
```

# Configurar partições Linux

Para configurar suas partições Linux, conclua a seguinte seção:

### Instalar provedores WBEM

Cada partição Linux deve ter provedores WBEM instalados. O WS-Man usa provedores comuns com o WBEM.

Para baixar e instalar os provedores WBEM, conclua as seguintes etapas:

1. Em um navegador, navegue até downloads.linux.hp.com/SDR/repo/bl920-wbem/.
2. Baixe os provedores para a sua versão do Linux e siga as instruções de instalação.

## Configurar partições Windows

Para configurar suas partições Windows, conclua as seguintes seções:

### Instalar provedores WBEM

Cada partição Windows deve ter provedores WBEM instalados. O WS-Man usa provedores comuns com o WBEM, enquanto o WinRM usa provedores comuns com o WMI.

Para baixar e instalar os provedores WBEM, conclua as seguintes etapas:

1. Em um navegador, navegue até www.hp.com/go/hpsc.
2. Digite **Servidor Superdome X** no campo de pesquisa e clique em **Ir**.
3. Clique no link **Drivers, softwares e firmwares**.
4. Clique no link **Servidor HP Superdome X**.
5. Na lista suspensa, selecione seu sistema operacional.
6. Expanda a seção **Software - Gerenciamento do sistema**, baixe os provedores e siga as instruções de instalação.

### Crie um certificado assinado

Para criar um certificado assinado, conclua as seguintes etapas:

1. Instale um certificado autoassinado. Use o método de sua escolha, ou use o seguinte método que utiliza o Microsoft Management Console:

   http://social.technet.microsoft.com/wiki/contents/articles/10377.create-a-certificate-request-using-microsoft-management-console-mmc.aspx
2. Como administrador, abra um prompt de comando e execute:

   ```
   winrm quickconfig –transport:https
   winrm set winrm/config/service/auth @{Basic=”true”}
   ```
3. Se o domínio do computador for um grupo de trabalho, você deverá adicionar o sufixo de domínio usado no nome comum quando criou o certificado:

a. Clique em **Iniciar**, clique com o botão direito em **Computador** e clique em **Propriedades**.
b. Em **Nome do computador, domínio e configurações do grupo de trabalho**, clique em **Alterar configurações**.
c. Na guia Nome do Computador, clique em **Alterar** e, em seguida, clique em **Mais**.
d. Adicione o sufixo DNS primário do computador.

# Adicionar credenciais de protocolo e iniciar a detecção

Você deve adicionar a credencial de logon do protocolo WS-Man para que o OA e todas as partições ao Insight RS Console para que o Insight RS possa se comunicar com esses pontos de extremidade.

Para detectar seus dispositivos monitorados, conclua as seguintes seções:

## Criar uma credencial de protocolo WS-Man para o OA no Insight RS Console

Para configurar o WS-Man no Insight RS Console, siga estas instruções:

1. Em um navegador da Web, faça logon no Insight RS Console.
2. No menu principal, selecione **Detecção** e clique na guia **Credenciais**.
3. Na lista suspensa **Selecionar e configurar protocolo**, selecione **Protocolo de gerenciamento de serviços da Web (WSMAN)**.
4. Clique em **Novo**. A caixa de diálogo Nova credencial é exibida.
5. Use a porta padrão: `443`.
6. Digite as credenciais de nome de usuário e senha que o Insight RS usará para se comunicar com o OA.
7. Clique em **Adicionar**.

## Criar uma credencial de protocolo WS-Man para as partições no Insight RS Console

**Observação:** As partições Windows usam o WinRM, que é a implementação do WS-Man da Microsoft. No Insight RS Console, configure um protocolo WS-Man para ambas as partições Linux e Windows.

Para configurar o WS-Man no Insight RS Console, siga estas instruções:

1. Em um navegador da Web, faça logon no Insight RS Console.
2. No menu principal, selecione **Detecção** e clique na guia **Credenciais**.
3. Na lista suspensa **Selecionar e configurar protocolo**, selecione **Protocolo de gerenciamento de**

**serviços da Web (WSMAN)**.

4. Clique em **Novo**. A caixa de diálogo Nova credencial é exibida.
5. Altere a porta padrão para: `5986`.
6. Digite os nomes de usuário e as senhas que o Insight RS usará para se comunicar com cada uma das partições.
7. Clique em **Adicionar**.

**Observação:** Crie credenciais adicionais do protocolo WS-Man se as suas partições usarem credenciais diferentes.

# Detectar o servidor Integrity Superdome X e as partições no Insight RS Console

Para detectar o servidor Integrity Superdome X e as partições no Insight RS Console, conclua as seguintes etapas:

1. Em um navegador da Web, faça logon no Insight RS Console.
2. No menu principal, selecione **Detecção** e clique na guia **Fontes**.
3. Expanda a seção Endereços IP e adicione os endereços IP dos OAs e das partições:
   a. Clique em **Novo**.
   b. Selecione **Endereço único**, **Intervalo de endereços** ou **Lista de endereços**.
   c. Digite os endereços IP dos OAs e das partições a serem detectados.
   d. Clique em **Adicionar**.
4. Clique em **Iniciar detecção**.

**Observação:** Se a detecção estiver configurada para detectar OAs em espera, ela irá preencher a tela dispositivos com o mínimo de informações sobre esses dispositivos, porque, apesar de suas interfaces de rede poderem estar ativas e alcançáveis, eles não estão monitorando a porta 443 usada para comunicações e, assim, não podem oferecem, ao Insight RS, informações sobre si mesmos. Da mesma forma, eles são dispositivos em espera com os quais o Insight RS não poderá estabelecer assinaturas de monitoramento diretamente. Se ocorrer um failover de OA, o OA irá passar a assinatura para o novo Monarch, e o Insight RS irá continuar a monitorar o OA, para ver se há indicações de eventos usando essa assinatura ativa.

# Verificar a detecção do Integrity Superdome X

Depois de concluída a detecção, selecione **Dispositivos** no menu principal. Verifique se todos os OAs do Integrity Superdome X e todas as partições previamente configurados para detecção foram detectados e se o status desses dispositivos mostra o ícone de êxito (✅).

## Verificar o OA do Integrity Superdome X

Para verificar as informações de dispositivos OA do Integrity Superdome X, conclua as seguintes etapas:

1. No Menu principal, selecione **Dispositivos**. Localize o OA do Integrity Superdome X e clique em seu nome de dispositivo.
2. Na guia **Dispositivo**, expanda a seção Status e verifique se o status do registro é **Registrado** e se Habilitado tem a opção **Sim** selecionada.
3. Expanda a seção Hardware e verifique se Nome de dispositivo, Categoria, Produto, Fornecedor, Endereço IP, Número de série adquirido e Número de produto adquirido estão preenchidos corretamente para o dispositivo. A categoria deve ser indicada como ***MANAGEMENT_DEVICE***, o Produto deve ser indicado como ***Superdome 2 16s x86*** e o Fornecedor deve ser ***hp***. Os valores restantes podem ser verificados usando as etapas para Telnet ou navegador da Web descritas acima.
4. Expanda a seção Garantia e contrato e verifique se os valores listados estão corretos.

**Observação:** Os campos Nome do SO e Versão do SO indicados para o OA estarão em branco se forem visualizados na seção Sistema operacional.

5. Expanda a seção Entrega e verifique se as informações estão corretas.

## Verificar as partições do Integrity Superdome X

Para verificar as informações de partições do Integrity Superdome X, conclua as seguintes etapas:

1. No Menu principal, selecione **Dispositivos**. Localize o OA do Integrity Superdome X e clique em seu nome de dispositivo.
2. Na guia **Dispositivo**, expanda a seção Status e verifique se o status do registro é Registrado e se Habilitado tem a opção Sim selecionada.
3. Expanda a seção Sistema operacional. Os campos Nome do SO e Versão do SO para a partição indicarão um Nome do SO e um número de Versão do SO que deve corresponder ao valor informado pelo comando `uname -r` quando este é inserido em uma conexão de janela SSH ou telnet com essa partição. Os valores indicados pela seção Hardware do SO devem ser os mesmos indicados na seção Hardware do OA detalhada acima. Expanda a seção Garantia e contrato e verifique se os valores listados estão corretos.
4. Expanda a seção Entrega e verifique se as informações estão corretas.

# Verificar a comunicação entre o dispositivo monitorado e o Insight RS

Para verificar a comunicação entre o dispositivo monitorado e o Insight RS, conclua as seguintes seções:

# Gerar eventos de teste

O Integrity Superdome X dá suporte à capacidade de um administrador se conectar ao OA e gerar uma indicação de teste WS-Man. Use o procedimento a seguir para gerar uma indicação de teste WS-Man:

1. Faça uma conexão Telnet ou SSH à interface CLI do OA e faça o logon usando uma conta de usuário com privilégios de administrador.
2. Digite o comando **test wsman**.
3. Em um navegador da Web, faça logon no Insight RS Console.
4. No menu principal, selecione **Eventos de serviços**. Clique duas vezes no cabeçalho da coluna Data, para que o evento mais recente apareça no topo, e verifique se o Insight RS recebeu o evento de teste.

Eventos de teste podem ser enviados das partições usando o System Management Homepage (SMH). Quando você envia um evento de teste, ele é transmitido pelo provedor de partições do SO e também pelo OA. Insight RS usa apenas o evento transmitido pelo caminho do OA. O provedor de partições do SO não transmite eventos informativos ao OA e, portanto, um evento de teste informativo não deve ser utilizado para essa etapa de verificação.

Para enviar um evento de teste de cada partição, conclua as seguintes etapas:

1. Abra um navegador da Web e conecte-se ao System Management Homepage (SMH) em execução na partição na porta `2381`. Faça logon usando uma conta de usuário com privilégios de administrador.
2. No SMH, navegue até **Configurações** → **Indicação de teste** e clique em **Enviar indicação de teste**.
3. Selecione *Aviso* ou *Erro* para o tipo de indicação de teste.
4. Clique em **Enviar**.
5. Em um navegador da Web à parte, faça logon no Insight RS Console.
6. No menu principal, selecione **Eventos de serviços**. Clique duas vezes no cabeçalho da coluna Data, para que o evento mais recente apareça no topo, e verifique se o Insight RS recebeu o evento de teste. Observe que eventos de partição são indicados por meio do OA e, por isso, você deve clicar no OA para visualizá-los. Para identificar qual partição originou o evento, abra o Evento de serviço clicando no link ID de evento, role para baixo até a seção Detalhes de host com falha e verifique se o valor indicado no campo FQDN preferido de host com falha: é o nome da partição e/ou se o valor indicado no campo IP do host com falha preferencial é o endereço IP usado para essa partição.

# Verificar coletas no Insight RS Console

Coletas não são executadas automaticamente depois da descoberta. A HP recomenda que você execute uma coleta manualmente após a descoberta completa para verificar a conectividade. Execute o cronograma de coleta manualmente na guia Serviços de coleta → Agendamentos de coleta. Para obter mais informações sobre o agendamento de coletas, consulte a Ajuda do Insight RS.

Verifique se essa coleta foi bem-sucedida na guia Serviços de coleta → Resultados da coleta básica do Insight RS Console.

1. Faça logon no Insight RS Console.
2. No menu principal, selecione **Serviços de coleta** e depois clique na guia **Resultados da coleta básica**.
3. Expanda a seção Coleta de configurações básicas do servidor.
4. Localize a entrada referente ao seu dispositivo e verifique a coluna Resultado. Se a coleta tiver sido bem-sucedida, um ícone de êxito será exibido (). Se ocorrer uma falha, um ícone de erro será exibido ().

# Se desejar, configure o Integrity Superdome X como uma solução

Para adicionar seu Integrity Superdome X ao Insight RS como uma solução, conclua as seguintes etapas:

1. No menu principal, selecione **Gerenciador de soluções**.
2. No painel Lista de soluções, clique em **Adicionar nova solução**. Os campos que precisam ser preenchidos aparecem no painel Criar nova solução.
3. No painel Criar nova solução, preencha os seguintes campos:

| Campo | Ação |
|---|---|
| **Nome da solução** | Digite um nome exclusivo para a solução. |
| **Tipo de solução** | Selecione uma solução na lista suspensa de soluções compatíveis da HP.<br><br>Essa seleção preencherá os campos Número de produto da solução e Modelo de produto da solução. Se você selecionar Outro, deverá preencher esses campos. |
| **Número de série da solução** | Digite o número de série da solução, localizado na etiqueta do hardware ou nas informações de pedido na ocasião em que você adquiriu a solução da HP. |
| **Número de produto da solução** | O número de produto da solução é automaticamente preenchido com base na seleção feita na lista suspensa Tipo de Solução. |
| **Modelo de produto da solução** | O modelo de produto da solução é automaticamente preenchido com base na seleção feita na lista suspensa Tipo de Solução. |
| **ID de entrega personalizada** | Digite o valor alfanumérico opcional que apenas será exigido se tiver sido fornecido a você pelo representante da HP ou nas instruções de configuração para fins de manuseio personalizado ou encaminhamento de eventos de serviço enviados à HP. |

4. Clique em **Salvar**. O sistema cria e exibe a nova solução no painel Lista de soluções. É exibido o painel de dispositivos atribuídos, no qual você pode atribuir dispositivos à nova solução.
5. Atribua dispositivos ou partições no painel de dispositivos atribuídos. A exibição padrão mostra dispositivos não atribuídos à solução. Para mostrar dispositivos adicionais, clique nas opções **Não atribuído a esta solução** ou **Todos os dispositivos**. Para mostrar dispositivos em um grupo de dispositivos específico, selecione um grupo de dispositivos na lista suspensa **Filtrar por grupo de**

**dispositivos**. Para procurar um dispositivo específico, digite o nome do dispositivo na caixa **Pesquisar**. A tabela mostra os dispositivos, com base nos seus critérios de filtro e pesquisa.

- Para adicionar um dispositivo, marque a caixa de seleção ao lado dele na tabela de dispositivos.
- Para remover um dispositivo, desmarque a caixa de seleção ao lado dele na tabela de dispositivos.

6. Clique em **Salvar dispositivos**.

O sistema cria e exibe a solução no painel Lista de soluções.

# Capítulo 14: Configurar servidores OpenVMS

**Importante:** Coletas de configuração para o OpenVMS no AlphaServer não estão disponíveis, exceto quando o servidor OpenVMS faz parte de uma coleta de SAN.

**Importante:** A HP fornece apenas suporte remoto limitado para clientes que estejam utilizando servidores HP Alpha. Assim como ocorre com o suporte padrão, o HP Insight Remote Support versão 7.x tentará detectar esses produtos como sendo produtos da HP monitorados remotamente e enviará informações sobre eventos de falha para a HP.

Entretanto, se houver problemas na operação dos recursos de monitoramento remoto do HP Insight Remote Support versão 7.x para esses produtos específicos, incluindo a detecção remota ou o envio de relatórios de eventos de falha para a HP, a HP resolverá esses problemas da melhor maneira possível comercialmente, mas sem garantia de resposta imediata ou resolução. Se um evento de falha for recebido com êxito pela HP, ele será gerenciado de acordo com o contrato de nível de suporte.

## Atender aos requisitos de configuração

Para configurar servidores OpenVMS de forma que eles sejam monitorados pelo Insight RS, conclua as seguintes seções:

**Tabela 14.1** ***Etapas de configuração do servidor OpenVMS***

| Tarefa | Concluída? |
|---|---|
| Certifique-se de que o Insight RS suporte seu servidor OpenVMS, verificando o *Notas de Lançamento do HP Insight Remote Support*. | |
| Instale e configure o ELMC para OpenVMS no servidor OpenVMS. | |
| Adicione o ELMC ao Insight RS Console. | |
| Detecte o servidor OpenVMS no Insight RS Console. | |
| (Opcional) Configure a resiliência do processador dinâmico (somente para servidores Integrity). | |

## Instalar e configurar o software de comunicação em servidores

Para configurar seus dispositivos monitorados, conclua as seguintes seções:

## Atender aos requisitos do sistema ELMC

Os dispositivos monitorados OpenVMS devem atender aos requisitos abaixo antes de o ELMC ser instalado. Nos clusters, os requisitos mínimos aplicam-se a cada nó no cluster.

## Atender aos requisitos de hardware e software

- Arquitetura do processador:
  - Servidor Integrity (Itanium)
  - HP AlphaServer
- Sistema operacional:
  - OpenVMS Itanium (Integrity) — 8.3-1H1 ou superior.

**Observação:** Algumas plataformas OpenVMS com suporte exigem uma versão mínima do 8.4. Consulte http://h71000.www7.hp.com/openvms/hw_supportchart.html.

**Observação:** A engenharia de apoio da HP mantém um programa de suporte para o sistema operacional OpenVMS. A HP não se compromete a oferecer suporte para o Insight Remote Support quando este é instalado em uma versão de sistema operacional que ultrapassou sua data de término de suporte. Para mais informações, acesse: http://www.hp.com/hps/os/os_pvs_amap.html.

  - OpenVMS AlphaServer — 7.3-2 ou superior
- Mínimo de 20.000 blocos de espaço livre em disco.
- Conectividade: O TCP/IP deve estar instalado e em execução.

  Mesmo que o tráfego TCP/IP para outras máquinas tenha sido desabilitado, a capacidade de resolver o nome do host local para um endereço IP deve estar habilitada. Caso contrário, o Director não consegue lidar com o tráfego de mensagens ELMC corretamente e não se inicia.

  O ELMC oficialmente suporta apenas um produto TCP/IP para OpenVMS: O HP TCP/IP Services para OpenVMS, versão 5.4 ou superior.

**Observação:** Outros produtos TCP/IP podem funcionar no estado em que estão. Portanto, a instalação do Insight Remote Support sempre é concluída, independentemente de qual produto TCP/IP estiver instalado, se houver algum.

- Entrada LOCALHOST: Para que o ELMC opere corretamente, a entrada LOCALHOST deve ser definida no banco de dados OpenVMS TCP/IP HOSTS. Ela é definida corretamente por padrão, mas pode ser removida, causando falhas no Insight Remote Support.

  Digite o seguinte comando:

  ```
  $ TCPIP SHOW HOST /LOCAL
  ```

  Procure LOCALHOST, que deve ter um endereço IP de 127.0.0.1. Se LOCALHOST não aparecer na lista, digite o seguinte comando:

  ```
  $ TCPIP SET HOST LOCALHOST /ADDRESS=127.0.0.1 /ALIAS=LOCALHOST
  ```

  Digite um comando ping para verificar se o LOCALHOST foi adicionado:

  ```
  $ TCPIP PING LOCALHOST
  PING LOCALHOST (127.0.0.1): 56 data bytes
  ```

```
64 bytes from 127.0.0.1: icmp_seq=0 ttl=64 time=0 ms
64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0 ms
64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0 ms
```

Depois de verificar que o `LOCALHOST` responde ao comando ping, use **Ctrl-C** ou **Ctrl-Y** para interromper o comando.

- Firmware do sistema: O pré-requisito de firmware do sistema oferece suporte ao registro em log de eventos de acordo com a especificação da tabela FRU versão 5, que é necessária para o processamento da árvore de configuração FRU do Insight Remote Support.

  Todos os sistemas DSxx e ES40 devem ter firmware V5.7-4 ou superior.

  Todos os outros produtos com suporte pelo Insight Remote Support vêm com uma versão de firmware compatível.

  Em geral, os usuários devem aproveitar as recentes melhorias obtendo a versão de firmware mais recente disponível para suas plataformas.

# *Atender a permissões e acessos necessários*

## *Conceder permissões necessárias para instalar o ELMC*

Para instalar ou desinstalar o ELMC, o usuário precisa de todos os privilégios OpenVMS abaixo:

- ALTPRI
- BUGCHK
- BYPASS
- CMKRNL
- DIAGNOSE
- IMPERSONATE
- NETMBX
- OPER
- SYSLCK
- SYSPRV
- TMPMBX

Ao desinstalar o ELMC, o usuário que executa a desinstalação deve usar o mesmo nome originalmente usado para instalar o ELMC.

O comando **set process** define privilégios para todos os nós do cluster quando o cluster é servido por apenas um disco do sistema. No entanto, em um cluster com vários discos de sistema, é possível optar por instalar o ELMC em nós servidos por outros discos do sistema além do que serve o nó a partir do qual está sendo feita a instalação. Neste caso, **set process** não estabelece privilégios sobre estes outros nós (os nós servidos pelos outros discos do sistema) e o ELMC não instala corretamente nestes outros nós.

Para instalar corretamente em clusters com diversos discos do sistema, configure os privilégios necessários como padrão (os privilégios obtidos ao fazer logon) em todos os nós onde desejar instalar o ELMC, em vez de usar o comando **set process**.

Consulte a seção "Instalação do pacote de software ELMC OpenVMS no dispositivo monitorado", para mais precauções sobre um disco do sistema em comparação com diversos discos do sistema.

## *Conceder permissões necessárias para executar o ELMC*

Para executar qualquer comando ELMC, o usuário precisa de todos os privilégios OpenVMS abaixo. Observe que estes privilégios são um subconjunto daqueles necessários para instalar, atualizar ou desinstalar o ELMC:

- ALTPRI
- BUGCHK
- CMKRNL
- DIAGNOSE
- IMPERSONATE
- NETMBX
- SYSPRV
- TMPMBX

## *Conceder acesso ao nó do cluster para o diretório de instalação do ELMC*

O pacote de instalação só pode se instalar em nós de cluster que tenham acesso ao diretório de destino onde será instalado o ELMC. Outra forma de explicar isso é que os nós devem montar o disco que contém o diretório de destino. Isso significa que uma instalação nem sempre pode colocar o ELMC em todos os nós do cluster, uma vez que todos os nós podem não ser capazes de identificar o local onde o ELMC está sendo instalado.

A situação é ilustrada da seguinte forma:

- **Cluster**: Todos os nós compartilham o mesmo disco do sistema.

  **Nó de instalação**: Qualquer nó.

  **Destino da instalação**: O local padrão SYS$COMMON:[HP...].

  **Resultado**: O ELMC se instala para todos os nós.
- **Cluster**: Com exceção de dois nós, todos compartilham o disco do sistema A. Os outros dois compartilham o disco do sistema B.

  **Nó de instalação**: Um nó que utiliza o disco do sistema A.

  **Destino da instalação**: O local padrão SYS$COMMON:[HP...].

  **Resultado**: Os outros dois nós não terão o ELMC.

No caso anterior, é possível instalar o ELMC mais uma vez para os dois nós restantes, executando a instalação a partir de qualquer nó e, novamente, escolhendo o local padrão SYS$COMMON:[HP...]. Considere isso uma instalação ELMC completamente separada da primeira instalação na maioria dos nós.

- **Cluster**: Com exceção de dois nós, todos compartilham o disco do sistema A. Os outros dois compartilham o disco do sistema B. Todos os nós também montam um disco C, que não é do sistema.

  **Nó de instalação**: Qualquer nó.

  **Destino da instalação**: Um diretório no disco C, especificado por você durante a instalação.

  **Resultado**: O ELMC se instala para todos os nós.

**Observação:** Em todos os casos o pacote de instalação também permite escolher apenas um subconjunto de nós que podem ver o local de instalação.

## *Arquivar e limpar o log de erros*

Depois que o Insight Remote Support estiver instalado no dispositivo host, ele usará o ELMC para analisar todos os eventos armazenados no log de erros, o que pode resultar em um alto uso da CPU por um longo período. Para controlar essa operação, recomendamos arquivar e limpar o log de erros antes de instalar. Isso reduz o tamanho do log e o tempo necessário para a verificação inicial.

Siga estas diretrizes para limpar o log de erros. Se o ELMC estiver instalado e funcionando durante a limpeza do log, não será necessário parar e reiniciar o processo Director. Além disso, não pare e reinicie o processo de registro de eventos do sistema `ERRFMT`.

`O registro de` erro padrão, normalmente SYS$SYSROOT:[SYSERR]ERRLOG.SYS, aumenta de tamanho e permanece no disco do sistema até que o usuário explicitamente o renomeie ou exclua. Quando um dos dois ocorre, o sistema cria um novo arquivo de registro de erro limpo após cerca de 15 minutos.

**Cuidado:** Depois de renomear ou excluir o registro existente, não instale o ELMC até que o novo registro padrão esteja presente.

Se o registro for renomeado, o registro salvo pode ser analisado posteriormente.

Além de começar com um log limpo antes de instalar o Insight Remote Support, talvez você queira realizar uma manutenção regular no log de erros. Um método é renomear o arquivo `errlog.sys` diariamente. Por exemplo, pode-se renomear o `errlog.sys` para `errlog.old` todas as manhãs, às 9h00. Para liberar espaço no disco do sistema, e então pode ser feito o backup da versão renomeada em um volume diferente e apagar o arquivo do disco de sistema.

## *Verificar o número de série*

Nos sistemas AlphaServer GS80, GS160 e GS320, verifique o número de série, como indicado antes de instalar o ELMC no dispositivo monitorado.

Determinados sistemas GS80, GS160, GS320 e não têm seu número de série do sistema definido corretamente na fábrica, e o Insight RS só funciona quando o número de série está configurado corretamente. Os números de série afetados começam com a letra "G".

No prompt do console do firmware do SRM (o prompt de quando o sistema é ligado), verifique o número de série com o seguinte comando:

```
show sys_serial_num
```

O número de série apresentado deve corresponder ao número de série real na etiqueta número do modelo/série, localizada no gabinete de alimentação. Se necessário, altere o número de série com o seguinte comando:

```
set sys_serial_num
```

Digite o número de série de seis caracteres fornecidos na etiqueta do gabinete de alimentação.

**Observação:** Esse problema também pode surgir quando diversos AlphaServers são pedidos, porque a fábrica pode atribuir um número de série idêntico para todos os sistemas. Neste cenário, o Insight RS não funciona corretamente, porque requer que cada AlphaServer tenha um número exclusivo. Se este for o caso, identifique cada AlphaServer, incluindo –1, –2, –3, e assim por diante, aos números de série, quando usar o comando **set sys_serial_num**.

**Observação:** Várias partições no mesmo AlphaServer sempre têm o mesmo número de série porque residem na mesma máquina. Não há conflitos do Insight RS nesse caso. Não tente atribuir números de série únicos para partições diferentes na mesma máquina.

# Instalar o pacote de software ELMC OpenVMS no dispositivo monitorado

Um cluster OpenVMS pode conter nós servidos por um disco do sistema comum, ou nós servidos por diversos discos do sistema. Todo nó é servido por um disco do sistema único, mas um disco do sistema pode servir um ou mais nós. Cada disco do sistema contém seu banco de dados PCSI próprio (registro do produto).

O ELMC pode ser instalado em um disco do sistema ou em um disco compartilhado que não é do sistema. No entanto, um disco compartilhado que não é do sistema pode ser acessado por diversos nós servidos por diferentes discos do sistema. Isso significa que o ELMC não está limitado a ser instalado apenas em nós servidos por um determinado disco do sistema. Um banco de dados PCSI, no entanto, é limitado a um disco do sistema.

Esse cenário pode gerar discrepâncias no comando **product show product wccproxy**. O comando sempre mostra o ELMC como instalado quando é executado a partir de um nó servido pelo mesmo disco do sistema do nó no qual o ELMC foi originalmente instalado (o nó da instalação). Isso porque o instalador do ELMC o registra apenas na base de dados PCSI para o disco do sistema que serve o nó da instalação, e não em qualquer outra base de dados PCSI. Isso pode resultar em dois tipos de informação enganosa:

- Se um nó é servido pelo mesmo disco do sistema do nó de instalação, mas o usuário não adicionar o ELMC a este nó, o comando mostra que o ELMC está instalado quando, na verdade, não está.

- Inversamente, se um nó é servido por um disco do sistema diferente daquele do nó da instalação e o usuário adicionou o ELMC a este nó, o comando não mostra que o ELMC está instalado quando, na verdade, ele está.

Se o ELMC já estiver instalado no servidor OpenVMS, certifique-se de que sua versão seja a 6.2 ou mais recente. Se a versão for anterior à 6.2, será preciso atualizá-la. Para verificar a versão do ELMC, execute o seguinte comando:`wccproxy version`.

Para instalar o pacote de software do ELMC, conclua as seguintes etapas:

1. No Insight RS Console, navegue até a guia **Configurações do administrador** → **Atualizações de software** e selecione o pacote de software *Coletor de Monitoramento do Log de Eventos (ELMC)*.
2. Na guia **Versão disponível**, clique em **Download**.
3. Quando o download for concluído, clique em **Instalar**. Os pacotes do ELMC são guardados na pasta `%HP_RS_DATA%\ELMC`. Por padrão, a pasta é `C:\ProgramData\HP\RS\DATA\ELMC`.

**Observação:** A pasta `ProgramData` é uma pasta oculta. Para exibir essa pasta, defina as opções de pasta para mostrar pastas ocultas.

4. Copie o pacote de software OpenVMS Itanium ELMC (`ELMC[`*`versão`*`]_OVMSI64.EXE`) para o dispositivo monitorado OpenVMS. Coloque o arquivo `.exe` em um diretório vazio. Verifique se:
   - Não há outros kits no diretório, especialmente outras versões de kits ELMC.
   - Não há arquivos ELMC ou WCCProxy antigos no diretório deixados de operações anteriores.
5. Extraia os arquivos de instalação do ELMC:

   **`$ run ELMC[`*`versão`*`]_OVMSI64.EXE`**
6. Execute o comando de instalação e siga os prompts:

   **`$ @wccproxy_install install`**

**Observação:** O comando executa o script DCL `wccproxy_install.com` no diretório atual. Não execute o comando **product install wccproxy**, que normalmente seria usado para instalar um produto baseado em PCSI. Esse comando interrompe e solicita a execução do script`wccproxy_install.com`. Defina o diretório padrão como o que contém o arquivo `wccproxy_install.com`, criado pela extração do arquivo ELMC `.exe` na etapa anterior.

O kit será instalado e encerrado sem prompts ao usuário. Quando o prompt DCL ($) retornar, a instalação terá sido concluída e o processo ELMC (WCCProxy) estará em execução.

# Configurar a resiliência do processador dinâmico

A resiliência do processador dinâmico, também conhecida como indicação de CPU, é a habilidade de o HP Insight Remote Support detectar várias condições de erro no processador ou no barramento/links do processador e tirar o processador de operação. Em servidores HP Integrity com HP OpenVMS, essa capacidade é implementada por uma combinação de análises dentro do HP Insight Remote Support e dos serviços de indicação de CPU do Kernel fornecidos pelo sistema operacional HP OpenVMS. Quando uma CPU é indicada, o serviço de indicação de CPU do Kernel remove o processador do conjunto ativo. Além

disso, o Insight Remote Support irá registrar uma chamada de serviço no log. A remoção do processador com falha do conjunto ativo evita que o processador apresente uma falha fatal no futuro. O registro automático da chamada de serviço permite reparos proativos automáticos, contribuindo ainda mais para a rápida solução do problema.

Para usar a resiliência do processador dinâmico, ela precisa estar configurada no servidor OpenVMS e também habilitada no Insight RS Console.

Para habilitar a resiliência do processador dinâmico no servidor OpenVMS, siga estas instruções:

1. Edite o procedimento de comando `SYS$INDICTMENT_POLICY.COM` e altere seus valores de 0 para 1:

   **`$ DEFINE/SYSTEM/EXECUTIVE_MODE/NOLOG SYS$INDICT_START 1`**

   **`$ DEFINE/SYSTEM/EXECUTIVE_MODE/NOLOG SYS$INDICT_ALLOW_CPUS 1`**

   Isso habilita todas as CPUs a serem elegíveis para Indicação, exceto a CPU 0.

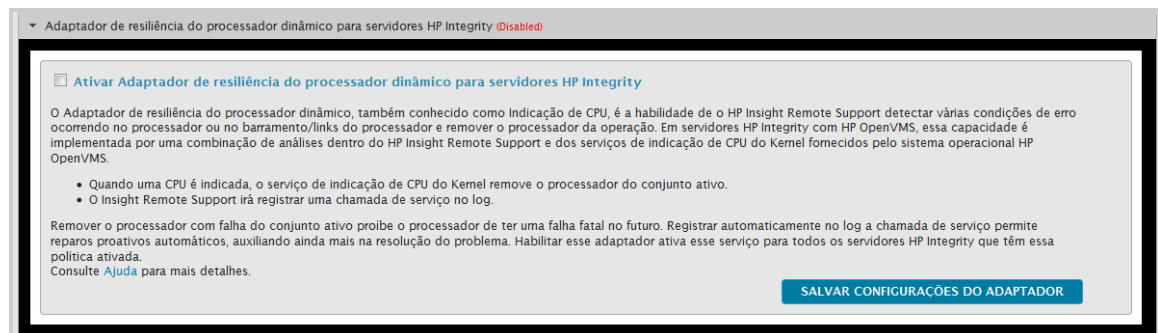
   **Observação:** A CPU 0 não pode ser removida. Se você quiser que algumas CPUs não sejam elegíveis, consulte a documentação do OpenVMS sobre o serviço de indicação, para saber como modificar esse procedimento de modo a atender suas necessidades.

2. Reinicie o servidor, para as alterações terem efeito.

   Quando o servidor de indicação for iniciado, aparecerá um processo `INDICT_SERVER` na saída de SHOW SYS:

```
ES47S3_V8.3>>sho sys
OpenVMS V8.3 on node ES47S3 17-NOV-2008 15:29:15.48 Uptime 0 00:13:01
Pid Process Name State Pri I/O CPU Page flts Pages
0000041C INDICT_SERVER HIB 8 6 0 00:00:00.00 79 95
```

Para habilitar o Dynamic Processor Resilience Adapter no Insight RS Console, conclua as seguintes etapas:

1. No menu principal, selecione **Configurações do administrador**.
2. Clique na guia **Adaptadores de integração**.
3. Clique no título **Dynamic Processor Resilience Adapter para servidores HP Integrity** para expandir o painel do adaptador.

   


4. Marque a caixa de seleção **Habilitar Dynamic Processor Resilience Adapter para servidores**

**HP Integrity**.

5. Clique em **Salvar configurações do adaptador**.

O Insight Remote Support habilita o Dynamic Processor Resilience Adapter. (Habilitado) é exibido agora ao lado do Dynamic Processor Resilience Adapter para indicar que ele está habilitado.

## Definir configurações de firewall e porta

Para obter uma lista completa de requisitos de firewall e de porta para dispositivos monitorados, consulte o *Informe de Segurança do HP Insight Remote Support*, em: http://www.hp.com/go/insightremotesupport/docs.

# Adicionar credenciais de protocolo e iniciar a detecção

Para detectar seus dispositivos monitorados, conclua as seguintes seções:

## Criar um protocolo ELMC no Insight RS Console

Para configurar o ELMC no Insight RS Console, conclua as seguintes etapas:

1. Em um navegador da Web, faça logon no Insight RS Console.
2. No menu principal, selecione **Detecção** e clique na guia **Credenciais**.
3. Na lista suspensa **Selecionar e configurar protocolo**, selecione **Coletor de monitoramento do log de eventos (ELMC)**.
4. Clique em **Novo**. A caixa de diálogo Nova credencial é exibida.

O Insight RS cria a credencial de protocolo, que é exibida na tabela de credenciais.

## Detectar o dispositivo no Insight RS Console

Para detectar o dispositivo por meio do Insight RS Console, conclua as seguintes etapas:

1. Em um navegador da Web, faça logon no Insight RS Console.
2. No menu principal, selecione **Detecção** e clique na guia **Fontes**.
3. Expanda a seção Endereços IP e adicione o endereço IP do seu dispositivo:
   a. Clique em **Novo**.
   b. Selecione **Endereço único**, **Intervalo de endereços** ou **Lista de endereços**.
   c. Digite os endereços IP dos dispositivos a serem detectados.
   d. Clique em **Adicionar**.
4. Clique em **Iniciar detecção**.

## Verificar o status de detecção e do dispositivo

Para verificar se o dispositivo foi detectado corretamente, conclua as seguintes etapas:

1. Em um navegador da Web, faça logon no Insight RS Console.
2. No menu principal, selecione **Dispositivos** e clique na guia **Resumo do dispositivo**.
3. Verifique se a coluna Status contém um ícone de êxito ( ).

   Se não houver ícone de êxito, tente descobrir que coluna está com problema e consulte a Ajuda on-line para informações de solução de problemas.

# Verificar a comunicação entre o dispositivo monitorado e o Insight RS

Para verificar a comunicação entre o dispositivo monitorado e o Insight RS, conclua a seguinte seção:

## Verificar coletas no Insight RS Console

Coletas não são executadas automaticamente depois da descoberta. A HP recomenda que você execute uma coleta manualmente após a descoberta completa para verificar a conectividade. Execute o cronograma de coleta manualmente na guia Serviços de coleta → Agendamentos de coleta. Para obter mais informações sobre o agendamento de coletas, consulte a Ajuda do Insight RS.

Verifique se essa coleta foi bem-sucedida na guia Serviços de coleta → Resultados da coleta básica do Insight RS Console.

1. Faça logon no Insight RS Console.
2. No menu principal, selecione **Serviços de coleta** e depois clique na guia **Resultados da coleta básica**.
3. Expanda a seção Coleta de configurações básicas do servidor.
4. Localize a entrada referente ao seu dispositivo e verifique a coluna Resultado. Se a coleta tiver sido bem-sucedida, um ícone de êxito será exibido ( ). Se ocorrer uma falha, um ícone de erro será exibido ( ).

# Capítulo 15: Configurar servidores Tru64 UNIX

**Importante:** Coletas de configuração para o Tru64 no AlphaServer não estão disponíveis, exceto quando o servidor Tru64 faz parte de uma coleta de SAN.

**Importante:** A HP fornece apenas suporte remoto limitado para clientes que estejam utilizando servidores HP Alpha. Assim como ocorre com o suporte padrão, o HP Insight Remote Support versão 7.x tentará detectar esses produtos como sendo produtos da HP monitorados remotamente e enviará informações sobre eventos de falha para a HP.

Entretanto, se houver problemas na operação dos recursos de monitoramento remoto do HP Insight Remote Support versão 7.x para esses produtos específicos, incluindo a detecção remota ou o envio de relatórios de eventos de falha para a HP, a HP resolverá esses problemas da melhor maneira possível comercialmente, mas sem garantia de resposta imediata ou resolução. Se um evento de falha for recebido com êxito pela HP, ele será gerenciado de acordo com o contrato de nível de suporte.

## Atender aos requisitos de configuração

Para configurar seus servidores Tru64 UNIX de forma que eles sejam monitorados pelo Insight RS, conclua as seguintes seções:

**Tabela 15.1** ***Etapas de configuração do servidor Tru64 UNIX***

| Tarefa | Concluída? |
|---|---|
| Certifique-se de que o Insight RS suporte seu servidor Tru64, verificando o *Notas de Lançamento do HP Insight Remote Support*. | |
| Instale e configure o ELMC para Tru64 no servidor Tru64 UNIX. | |
| Adicione o ELMC ao Insight RS Console. | |
| Detecte o servidor Tru64 no Insight RS Console. | |

## Instalar e configurar o software de comunicação em servidores

Para configurar seus dispositivos monitorados, conclua as seguintes seções:

### Atender aos requisitos do sistema ELMC

Os dispositivos monitorados Tru64 UNIX devem atender aos requisitos abaixo antes de o ELMC ser instalado. Nos clusters, os requisitos mínimos aplicam-se a cada nó no cluster.

## Requisitos de hardware e software

- Arquitetura do processador: HP AlphaServer
- Sistema operacional: Tru64 UNIX versão 4.0F, 4.0G, 5.1A ou superior

**Observação:** A engenharia de apoio da HP mantém um programa de suporte para o sistema operacional Tru64 UNIX. A HP não se compromete a oferecer suporte para o Insight Remote Support quando este é instalado em uma versão de sistema operacional que ultrapassou sua data de término de suporte.

- Mínimo de 20 MB de espaço livre em disco para a instalação de todos os componentes.
- Os serviços de TCP/IP devem estar instalados e em execução.
- Atualize para a V1.22 ou superior do driver Emulex (EMX) se for usado um adaptador EMX LP6000, LP7000 ou LP8000 (KGPSA-xx), por meio da interface de programação SLI2. O uso de um driver EMX anterior à versão V1.22 pode resultar em processamento incorreto de dados.
- Firmware do sistema: O pré-requisito de firmware do sistema oferece suporte ao registro em log de eventos de acordo com a especificação da tabela FRU versão 5, que é necessária para o processamento da árvore de configuração FRU do Insight Remote Support.
  - Todos os sistemas DSxx e ES40 devem ter firmware V5.7-4 ou superior.
  - Todos os outros sistemas (atualmente ES45, GSxx e TS202c) são fornecidos com uma versão de firmware compatível.

  Em geral, os usuários devem tirar partido das mais recentes melhorias, obtendo a versão de firmware mais recente disponível para suas plataformas.

## Permissões e acessos necessários

Para instalar, atualizar ou desinstalar o ELMC, é necessário estar logado como usuário root. O diretório `/usr/opt/hp/svctools` é de propriedade do root, e tem permissões rwx (ler, escrever e executar) para o root (proprietário) e nenhuma permissão para qualquer outro usuário (grupo ou mundial).

## Arquivar e limpar o log de erros

Depois que o Insight Remote Support estiver instalado no dispositivo host, ele usará o ELMC para analisar todos os eventos armazenados no log de erros, o que pode resultar em um alto uso da CPU por um longo período. Para controlar essa operação, recomendamos arquivar e limpar o log de erros antes de instalar. Isso reduz o tamanho do log e o tempo necessário para a verificação inicial.

Siga estas diretrizes para limpar o log de erros. Se o ELMC estiver instalado e funcionando durante a limpeza do log, não será necessário parar e reiniciar o processo Director. Além disso, não pare e reinicie o processo de registro de eventos do sistema `ERRFMT`.

## Tru64 UNIX versão 4.0F

1. Interrompa o processo binlogd: **`# /sbin/init.d/binlog stop`**
2. Se desejar, mova o log de erros original para qualquer nome apropriado, por exemplo:

   **`# mv /var/adm/binary.errlog /var/adm/binary.errlog.2002_06_11`**

   Logs salvos podem ser analisados posteriormente.
3. Se você pulou a etapa 2, remova o log deerros original: **`# rm /var/adm/binary.errlog`**
4. Reinicie o servidor. Durante o reinício, o servidor cria um novo arquivo `binary.errlog` contendo um novo evento de configuração. O servidor também reinicia o processo `binlogd`.

## Tru64 UNIX versão 4.0G

1. Interrompa o processo binlogd: **`# /sbin/init.d/binlog stop`**
2. Se desejar, mova o log de erros original para qualquer nome apropriado, por exemplo:

   **`# mv /var/adm/binary.errlog /var/adm/binary.errlog.2002_06_11`**

   Logs salvos podem ser analisados posteriormente.
3. Se você pulou a etapa 2, remova o log deerros original: **`# rm /var/adm/binary.errlog`**
4. Reinicie o processo binlogd: **`# /sbin/init.d/binlog start`**

## Tru64 UNIX versão 5.A ou superior

Um novo recurso pode enviar um sinal ao binlogd para salvar o log atual e criar um novo, sem interromper o processo. Siga as instruções na seção "Verifique o CDSL binary.errlog" e na seção “Limpar o log com o binlogd em execução".

## Verifique o CDSL binary.errlog

Na versão 5.1A ou superior, o log de erros binário `/var/adm/binary.errlog` deve ser um link simbólico dependente de contexto (CDSL) apontando para um arquivo específico para cada nó do cluster. Isso garante que o processo binlogd em cada nó armazene os eventos daquele nó em seu log de erros específico para o nó `/var/cluster/members/<memb>/adm/binary.errlog`.

Se o CDSL for excluído, o binlogd o recria como um arquivo regular, comum ao cluster, o que não funciona corretamente. Para verificar o arquivo, execute o comando:

**`# ls -l /var/adm/binary.errlog`**

O resultado correto é semelhante ao seguinte:

```
>lrwxrwxrwx 1 root adm 43 Jun 11 12:54 /var/adm/binary.errlog -
>../cluster/members/<memb>/adm/binary.errlog
```

Um resultado incorreto não exibe o indicador de link ->:

```
-rw-r----- 1 root adm 560 Jun 11 12:59 /var/adm/binary.errlog
```

Se necessário, corrija o arquivo, seguindo estas instruções:

1. Pare o processo binlogd em todos os nós do cluster, com o seguinte comando em cada nó:

   ```
   # /sbin/init.d/binlog stop
   ```

2. Logs salvos podem ser analisados posteriormente. Se desejar, mova o log de erros original para qualquer nome apropriado, por exemplo:

   ```
   # cd /var/adm
   ```

   ```
    # mv binary.errlog binary.errlog.2002_06_11
   ```

3. Emita comandos de movimentação similares para os logs de erros específicos do nó que desejar salvar, por exemplo:

   ```
   # mv /var/cluster/members/<memb>/adm/binary.errlog
   /var/cluster/members/<memb>/adm/binary.errlog.2002_06_11
   ```

   ```
   # mv /var/cluster/members/<memb>/adm/binlog.saved/binary.errlog.saved
   /var/cluster/members/<memb>/adm/binlog.saved/binary.errlog.saved.2002_06_11
   ```

4. Remova os logs de erros existentes, ignorando qualquer erro do tipo `Arquivo ou diretório não encontrado`:

   ```
   # rm /var/adm/binary.errlog
   ```

   ```
   # rm /var/cluster/members/<memb>/adm/binary.errlog
   ```

   ```
   # rm /var/cluster/members/<memb>/adm/binlog.saved/binary.errlog.saved
   ```

5. Crie o CDSL:

   ```
   # mkcdsl /var/adm/binary.errlog
   ```

6. Reinicie o processo binlogd em todos os nós do cluster, com o seguinte comando em cada nó:

   ```
   # /sbin/init.d/binlog start
   ```

## *Limpar o log com binlogd em execução*

Para a versão 5.1A ou superior, siga estas instruções em cada nó do cluster que desejar limpar:

1. Verifique se a seção CDSL do `binary.errlog` está completa como descrito anteriormente.

2. Se desejar, evite que as cópias previamente salvas sejam substituídas movendo-as para qualquer nome apropriado, por exemplo:

   ```
   # cd /var/cluster/members/member/adm/binlog.saved
   ```

   ```
   # mv binary.errlog.saved binary.errlog.2002_06_11
   ```

3. Faça com que o binlogd copie e limpe o log de erros original:

   ```
   # kill -USR1 `cat /var/run/binlogd.pid`
   ```

   O comando anterior não mata o processo `binlogd`. Em vez disso, ele envia um sinal para o `binlogd` que faz com que ele copie `/var/adm/binary.errlog` para `/var/cluster/members/member/adm/binlog.saved`. Em seguida, o arquivo original `/var/adm/binary.errlog` é recriado com apenas um evento de configuração. Observe que

`/var/adm/binary.errlog` é um CDSL que aponta para
`/var/cluster/members/<memb>/adm/binary.errlog`.

Para mais detalhes, incluindo como automatizar esse tipo de gerenciamento de log de erros, consulte a seção sobre gerenciamento do arquivo de log de erros binário na página man do binlogd.

## *Verificar o número de série*

Nos sistemas GS80, GS160 e GS320, verifique o número de série como indicado antes de instalar o ELMC no dispositivo monitorado.

Determinados sistemas GS80, GS160 e GS320 não têm seu número de série do sistema definido corretamente na fábrica, e as regras de evento no dispositivo host só funcionam quando o número de série está configurado corretamente. Os números de série afetados começam com a letra "G".

No prompt do console do firmware do SRM (o prompt de quando o servidor é ligado), verifique o número de série com o seguinte comando:

```
show sys_serial_num
```

O número de série apresentado deve corresponder ao número de série real na etiqueta número do modelo/série, localizada no gabinete de alimentação. Se necessário, altere o número de série com o seguinte comando:

```
set sys_serial_num
```

Digite o número de série de seis caracteres fornecidos na etiqueta do gabinete de alimentação.

**Observação:** Esse problema também pode surgir quando diversos AlphaServers são pedidos, porque a fábrica pode atribuir um número de série idêntico para todos os sistemas. Neste cenário, as regras de eventos não funcionam corretamente porque eles exigem que cada AlphaServer tenha um número único. Se este for o caso, identifique cada AlphaServer, incluindo –1, –2, –3, e assim por diante, aos números de série, quando usar o comando **set sys_serial_num**.

Várias partições no mesmo AlphaServer sempre têm o mesmo número de série porque residem na mesma máquina. Não há conflitos nesse caso. Não tente atribuir números de série únicos para partições diferentes na mesma máquina.

# Instalar o pacote de software ELMC Tru64 UNIX

Primeiro, extraia o pacote de software ELMC; em seguida, instale-o.

Para extrair o kit de instalação ELMC, coloque o arquivo `.gz` do kit em um diretório temporário e descompacte-o:

```
# gunzip ELMC_<versão>.tar.gz
```

Em seguida, extraia o arquivo tar. Se já existir um subdiretório "kit" quando esse comando for executado, verifique se não existem arquivos de kits ELMC anteriores nesse subdiretório antes de executar o comando.

```
# tar -xvf ELMC_<versão>.tar
```

Esse comando cria um diretório kit (se já não existir) e extrai os arquivos de instalação ELMC.

**Observação:** Se for instalar em um ambiente TruCluster, garanta que todos os nós estejam em execução antes de continuar.

Quando seu diretório atual é aquele no qual foi extraído o kit, digite o seguinte comando para instalar os arquivos para o ELMC WCCProxy:

```
# setld -l kit
```

Não execute o comando `setld -D` para direcionar a instalação do ELMC a um diretório não padrão. O diretório padrão é obrigatório para o funcionamento adequado do ELMC.

O kit será instalado e encerrado sem prompts ao usuário. Quando for retornado o prompt do shell (#), a instalação terá sido concluída e o processo wccproxy estará em execução.

# Adicionar credenciais de protocolo e iniciar a detecção

Para detectar seus dispositivos monitorados, conclua as seguintes seções:

## Criar um protocolo ELMC no Insight RS Console

Para configurar o ELMC no Insight RS Console, conclua as seguintes etapas:

1. Em um navegador da Web, faça logon no Insight RS Console.
2. No menu principal, selecione **Detecção** e clique na guia **Credenciais**.
3. Na lista suspensa **Selecionar e configurar protocolo**, selecione **Coletor de monitoramento do log de eventos (ELMC)**.
4. Clique em **Novo**. A caixa de diálogo Nova credencial é exibida.

O Insight RS cria a credencial de protocolo, que é exibida na tabela de credenciais.

## Detectar o dispositivo no Insight RS Console

Para detectar o dispositivo por meio do Insight RS Console, conclua as seguintes etapas:

1. Em um navegador da Web, faça logon no Insight RS Console.
2. No menu principal, selecione **Detecção** e clique na guia **Fontes**.
3. Expanda a seção Endereços IP e adicione o endereço IP do seu dispositivo:
   a. Clique em **Novo**.
   b. Selecione **Endereço único**, **Intervalo de endereços** ou **Lista de endereços**.
   c. Digite os endereços IP dos dispositivos a serem detectados.

d. Clique em **Adicionar**.

4. Clique em **Iniciar detecção**.

## Verificar o status de detecção e do dispositivo

Para verificar se o dispositivo foi detectado corretamente, conclua as seguintes etapas:

1. Em um navegador da Web, faça logon no Insight RS Console.
2. No menu principal, selecione **Dispositivos** e clique na guia **Resumo do dispositivo**.
3. Verifique se a coluna Status contém um ícone de êxito ().

   Se não houver ícone de êxito, tente descobrir que coluna está com problema e consulte a Ajuda on-line para informações de solução de problemas.

# Verificar a comunicação entre o dispositivo monitorado e o Insight RS

Para verificar a comunicação entre o dispositivo monitorado e o Insight RS, conclua a seguinte seção:

## Verificar coletas no Insight RS Console

Coletas de configuração não têm suporte para esse tipo de dispositivo, exceto quando ele faz parte de uma coleta de SAN. Se você adicionou esse dispositivo a uma coleta de SAN, poderá executar manualmente uma coleta de SAN para verificar a configuração.

1. Faça logon no Insight RS Console.
2. No menu principal, selecione **Serviços de coleta**.
3. Clique na guia **Agendamentos de coleta**.
4. No painel Lista de agendamentos de coleta, selecione **Agendamento de coletas de configuração da SAN**. Informações sobre a coleta são exibidas no painel Informações da coleta. O painel Nestes dispositivos lista os dispositivos em que a coleta será executada.
5. No painel Informações de agendamento, clique em **Executar agora**.
6. Quando a coleta terminar, clique na guia **Resultados da Coleta de Armazenamento SAN**.
7. Expanda a seção Coleta de Configurações de SAN.
8. Localize a entrada referente ao seu dispositivo e verifique a coluna Resultado. Se a coleta tiver sido bem-sucedida, um ícone de êxito será exibido (). Se ocorrer uma falha, um ícone de erro será exibido ().

# Capítulo 16: Configurar servidores NonStop

O HP Insight Remote Support oferece suporte para sistemas NonStop, incluindo servidores HP Integrity NonStop NS-series, HP Integrity NonStop BladeSystems e servidores HP Integrity NonStop série X. Para obter detalhes, consulte o *Notas de Lançamento do HP Insight Remote Support*.

Em sistemas NonStop, o software NonStop OSM (Open System Management) realiza o diagnóstico de problemas e cria relatórios de incidentes (IRs). O OSM envia esses IRs para o Insight Remote Support, que, por sua vez, os encaminha para o suporte da HP.

**Observação:** Servidores NonStop ***não*** oferecem suporte a coletas de configuração.

Usar o Insight Remote Support no ambiente NonStop envolve requisitos e etapas de configuração específicas para o NonStop. Para obter informações sobre como começar, consulte o documento *Insight Remote Support for NonStop*. Ele está disponível no seguinte local: www.hp.com/go/nonstop-serviceinfo.

# Capítulo 17: Configurar servidores IBM

Insight Remote Support (RS) deve ser capaz de se comunicar com o servidor IBM para que ele possa ser monitorado. Insight RS pode se comunicar com servidores IBM executando o Windows com SNMP. As informações a seguir descrevem como instalar e configurar os protocolos de comunicação e outros componentes de software recomendados, de modo que possam ser monitorados pelo Insight RS.

Insight RS oferece suporte aos seguintes servidores IBM:

- IBM System x™ (xSeries®)
- Chassi IBM BladeCenter® e servidores BladeCenter®

**Observação:** Insight RS oferece suporte aos sistemas operacionais Microsoft Windows Server 2008 e 2008 R2 para servidores IBM.

**Importante:** Não há suporte para coletas de configuração.

## Atender aos requisitos de configuração

Para configurar servidores IBM de forma que eles sejam monitorados pelo Insight RS, conclua as seguintes seções:

**Tabela 17.1** ***Etapas de configuração do servidor IBM***

| Tarefa | Concluída? |
|---|---|
| Certifique-se de que o Insight RS suporte seu servidor IBM, verificando o *Notas de Lançamento do HP Insight Remote Support*. | |
| Configurar o serviço SNMP do Windows no servidor IBM. | |
| Instale o IBM Director Agent no servidor IBM. | |
| Configure o destino da interceptação SNMP e a cadeia de caracteres da comunidade de leitura SNMP. | |
| Adicione o protocolo SNMP ao Insight RS Console. | |
| Detecte o servidor IBM no Insight RS Console. | |
| Adicione o Tipo de suporte e o Identificador de suporte do dispositivo ao Insight RS Console. | |

## Instalar e configurar o software de comunicação em servidores

Para configurar seus dispositivos monitorados, conclua as seguintes seções:

# Configurar o serviço SNMP do Windows

1. No dispositivo monitorado, abra a janela Propriedades do serviço SNMP e selecione a guia **Interceptações**.

2. No campo **Nome da comunidade**, digite o nome da comunidade SNMP e clique em **Adicionar à lista**.

**Importante:** O nome da comunidade deve corresponder ao nome da comunidade configurado no Console do Insight RS.

3. No campo destinos das interceptações, adicione o dispositivo host à lista:
   a. Para abrir a janela Configuração do serviço SNMP, clique em **Adicionar**.
   b. Digite o nome de host ou o endereço IP do dispositivo host.
   c. Clique em **Adicionar**.
4. Clique na guia **Segurança** e verifique se o nome da comunidade foi adicionado à lista de nomes de comunidades Aceitos.

5. Marque a caixa de seleção **Enviar interceptação de autenticação**.
6. Clique em **Aceitar pacotes SNMP de qualquer host**.
7. Clique em **OK** para salvar as configurações.

# Instalar e configurar o SNMP

O IBM Director Agent deve ser instalado no servidor IBM, e o serviço SNMP deve ser configurado. O IBM Director Agent inclui um agente SNMP.

Em servidores Windows 2008 e 2008 R2, a solução foi testada com o IBM Systems Director Common Agent versão 6.1.1.

 **Importante:** Insight RS apenas oferece suporte à versão 6.1.1 do agente.

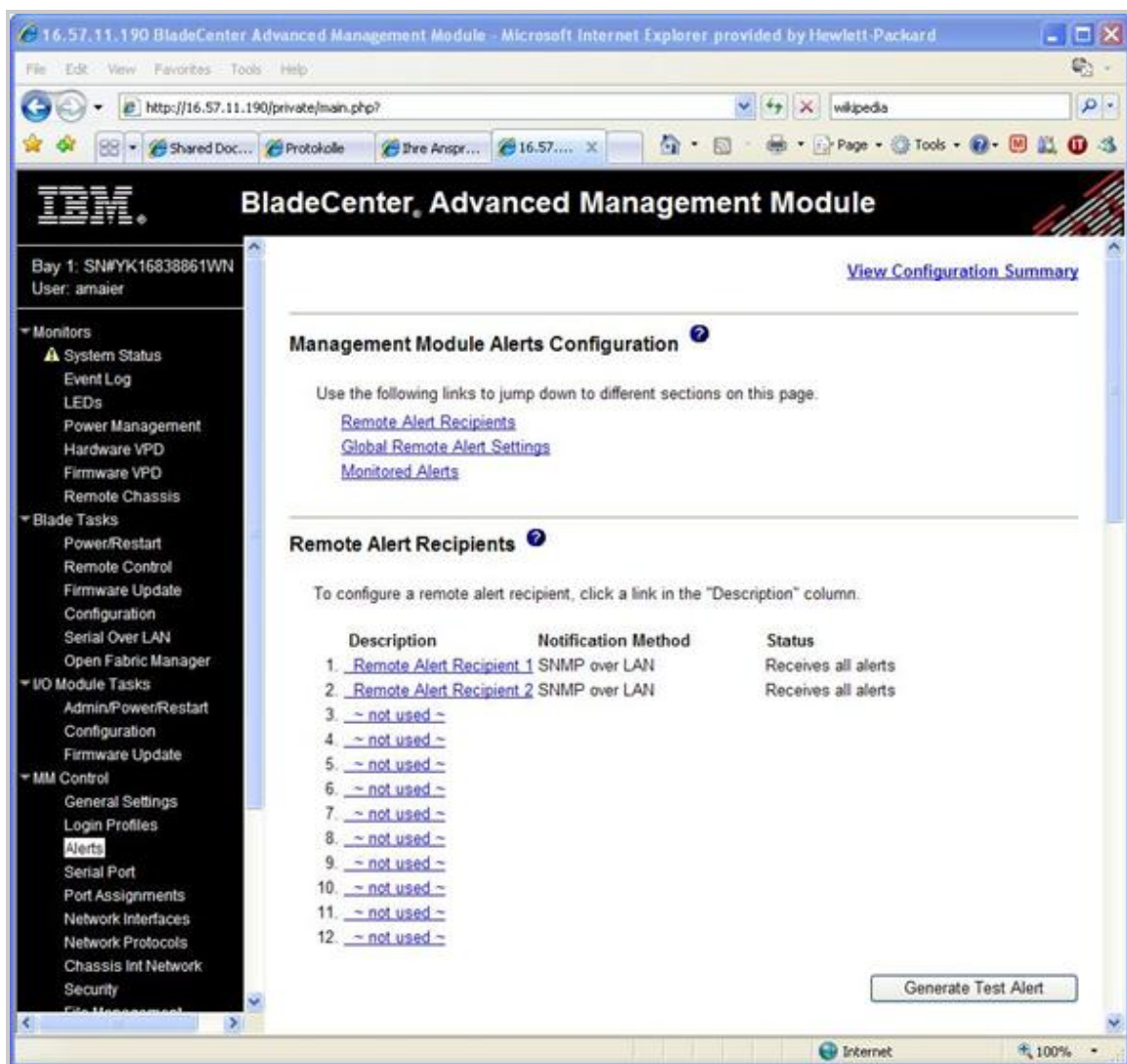
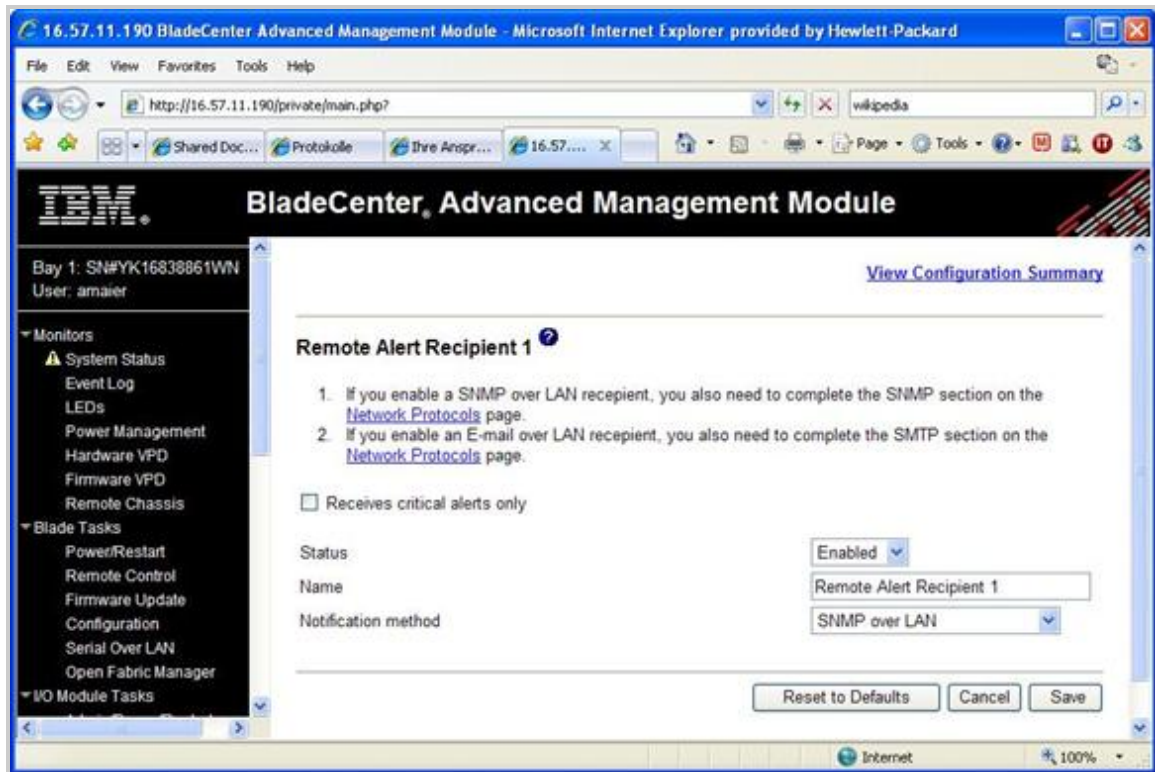
## *Instalar o IBM Director Agent*

Baixe e instale o IBM Director Agent ou o IBM Systems Director Common Agent para xSeries em: http://www-03.ibm.com/systems/director/downloads/agents.html.

**Observação:** Se um processador de serviço estiver instalado no servidor monitorado, conclua as seguintes etapas:

1. Para configurar o destino de interceptação do processador de serviço, use a tarefa de assistente do processador de gerenciamento, no console do IBM Director.
2. Adicione o endereço IP do dispositivo host como um destino de armadilha.
3. Reinicie o processador do serviço.

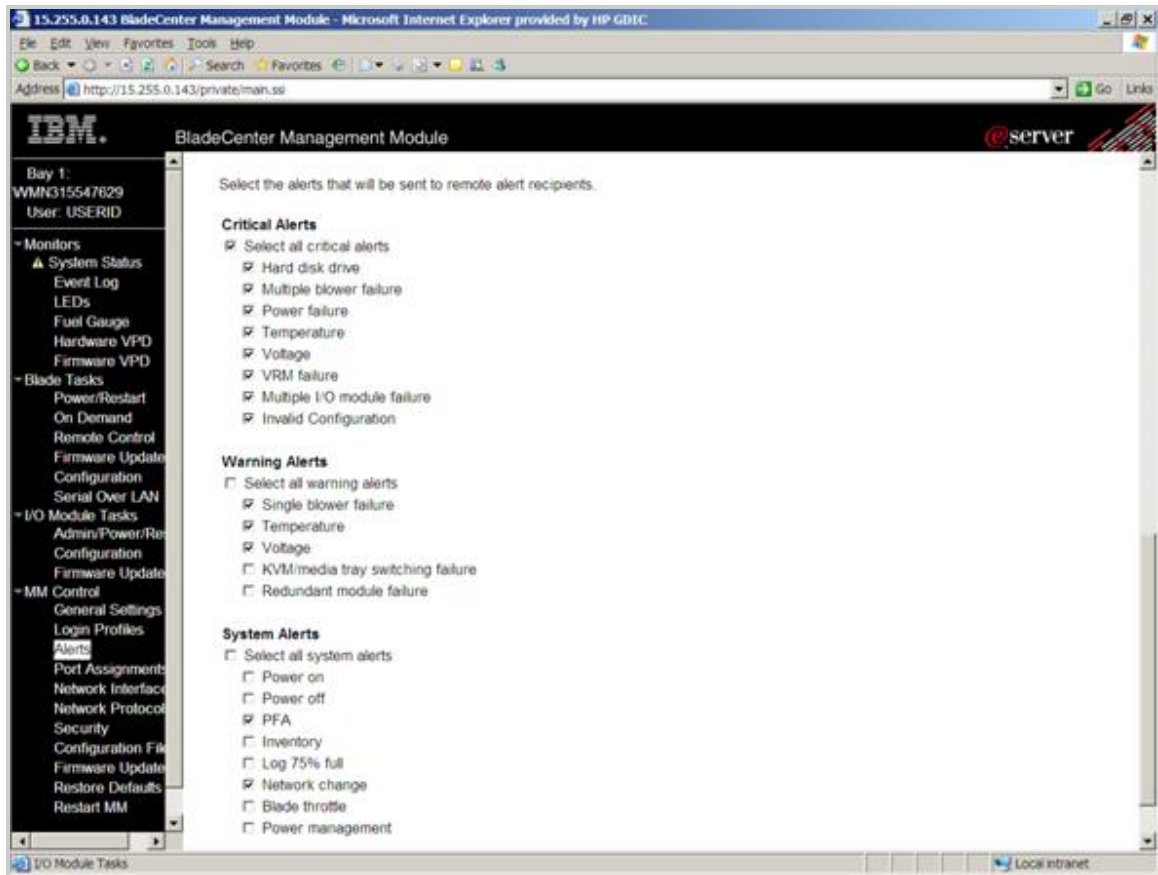
## *Configurar o Módulo de Gerenciamento do chassi IBM BladeCenter®*

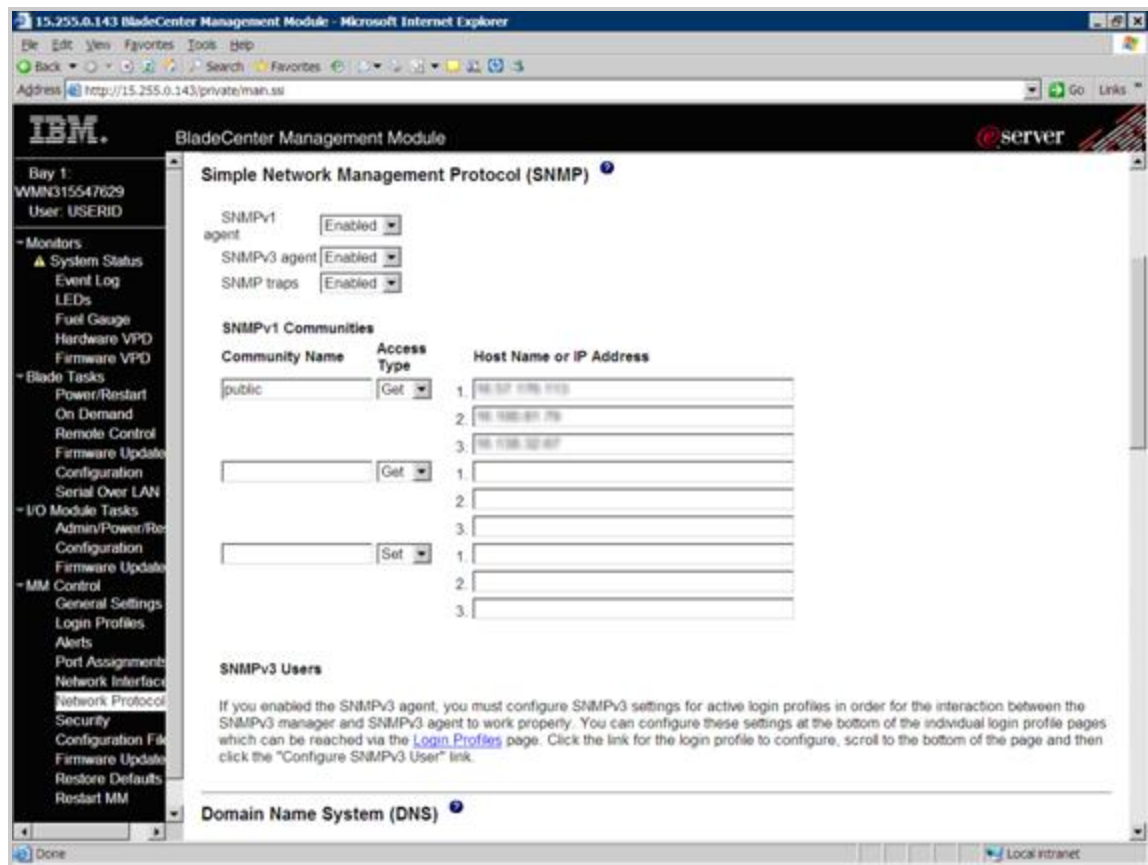
1. Faça login na página da Web do Módulo de Gerenciamento do BladeCenter.
2. Selecione os alertas na seção Controle MM do menu esquerdo. A página de Alertas aparece.

3. Selecione um dos itens não-utilizados na coluna Nome. A página Destinatário de Alerta Remoto aparece.

4. Na página Destinatário de Alerta Remoto:
   a. Na lista suspensa **Status**, selecione **Habilitado**.
   b. No campo Nome, digite um nome de Destinatário de Alerta Remoto. Por exemplo: Destinatário de Alerta Remoto 1
   c. Na lista suspensa **Método de notificação**, selecione **SNMP pela rede local**.
   d. No campo endereço IP ou nome de host, digite o endereço IP do dispositivo host.
   e. Opcional: No campo endereço de email, digite um endereço de email, se você quiser ser notificado sobre alertas por email
5. Selecione **Salvar**. A página de Alertas aparece. O Destinatário de Alerta Remoto salvo aparece na página Alertas do Módulo de Gerenciamento do BladeCenter.
6. Na página Alertas, role até a seção Alertas monitorados.
7. Selecione estas opções:
   a. Todos os alertas críticos
   b. De Alertas de aviso:
      i. Falha no dispositivo de refrigeração para um único chassi (ventoinha)
      ii. Temperatura
      iii. Tensão

c. De Alertas de sistema:

      i. PFA

      ii. Mudança de rede

8. Salve suas configurações.

9. Na seção Controle MM, no menu esquerdo, selecione **Protocolo de rede**. A página Protocolo de rede aparece.

10. Role a tela até SNMP.

11. Na lista suspensa **Agente SNMPv1**, selecione **Habilitado**.
12. Configure uma comunidade SNMPv1:
    a. No campo Nome da comunidade, digite um nome de comunidade SNMP.
    b. Na lista suspensa **Tipo de acesso**, selecione **Obter**.
    c. No campo Nome de host ou Endereço IP, digite o nome de host do dispositivo host ou endereço IP.
13. Clique em **Salvar**.
14. Reinicie o módulo de gerenciamento do BladeCenter:
    a. Na seção Controle MM, no menu esquerdo, selecione **Reiniciar MM**.
    b. Clique em **Reiniciar**.

# Instalar drivers de dispositivo IBM e firmware do processador de serviço

Para usar um dispositivo anexo, os drivers desse dispositivo devem estar instalados. Certifique-se de que os processadores de serviço do servidor IBM adequados estão instalados.

**Observação:**

- Para determinar que processadores de serviço estão instalados em um servidor IBM, consulte o documento *Implementar soluções de gerenciamento de sistema usando o IBM Director*, em: http://www.redbooks.ibm.com/redbooks/pdfs/sg246188.pdf
- Um driver de dispositivo combinado para todos os processadores de serviço está disponível de acordo com o sistema operacional em: http://www.ibm.com/systems/support/.
- Não são necessários drivers adicionais para servidores que tenham somente um processador ISM instalado.

Atualize o firmware do processador de serviço para a versão mais recente, para garantir que todos os recursos dos processadores de serviço estejam disponíveis.

Para instalar os drivers de dispositivo IBM, siga estas instruções:

1. Acesse: www.ibm.com/systems/support.
2. Na barra de navegação superior, selecione **Suporte & downloads**.
3. Na lista suspensa **Escolher tipo de suporte**, selecione **System x**.
4. Na lista de links populares, selecione Software e drivers de dispositivo.
5. Baixe e instale do driver de dispositivo para o seu servidor.
6. Reinicie o servidor (se solicitado).

# Adicionar credenciais de protocolo e iniciar a detecção

Para detectar seus dispositivos monitorados, conclua as seguintes seções:

## Criar uma credencial de protocolo SNMPv1 no Insight RS Console

Se a cadeia da comunidade SNMPv1 do dispositivo estiver definida como `pública` e o modo de acesso da comunidade for `somente leitura`, o Insight RS associará automaticamente um protocolo SNMP ao seu dispositivo. Se você usar uma cadeia de comunidade diferente ou uma porta não padrão, precisará criar uma credencial de protocolo SNMPv1 no Insight RS Console.

Para configurar o SNMPv1 no Insight RS Console, conclua as seguintes etapas:

1. Em um navegador da Web, faça logon no Insight RS Console.
2. No menu principal, selecione **Detecção** e clique na guia **Credenciais**.
3. Na lista suspensa Selecionar e configurar protocolo, selecione **Simple Network Management Protocol versão 1 (SNMPv1)**.
4. Clique em **Novo**. A caixa de diálogo Nova credencial é exibida.
5. Digite a cadeia de caracteres da comunidade configurada no seu dispositivo.
6. Clique em **Adicionar**.

O Insight RS cria a credencial de protocolo, que é exibida na tabela de credenciais.

# Detectar o dispositivo no Insight RS Console

Para detectar o dispositivo por meio do Insight RS Console, conclua as seguintes etapas:

1. Em um navegador da Web, faça logon no Insight RS Console.
2. No menu principal, selecione **Detecção** e clique na guia **Fontes**.
3. Expanda a seção Endereços IP e adicione o endereço IP do seu dispositivo:
   a. Clique em **Novo**.
   b. Selecione **Endereço único**, **Intervalo de endereços** ou **Lista de endereços**.
   c. Digite os endereços IP dos dispositivos a serem detectados.
   d. Clique em **Adicionar**.
4. Clique em **Iniciar detecção**.

# Configurar informações de garantia e contrato

Monitorar o suporte para servidores que não sejam da HP requer atenção especial aos dados de garantia e contrato do servidor. Os números de série e de produto que são detectados geralmente não combinam com os números de série e de produto listados no contrato de suporte HP.

Para configurar os números de série e de produto, siga estas instruções:

1. No Insight RS Console, verifique se o servidor é exibido na página Dispositivos.

   **Importante:** Para o chassi do IBM BladeCenter®, a coluna Produto fica vazia, por padrão.

2. Clique no **Nome do dispositivo** e, na guia **Dispositivo**, digite as seguintes informações:

   **Observação:** A equipe de suporte de conta da HP deve adicionar os dados de benefícios e para servidores IBM no Insight RS Console.

   - Número de série substituto (como listado no contrato)
   - Número de produto substituto (como listado no contrato)
   - Tipo de suporte
   - Identificador de suporte

# Verificar o status de detecção e do dispositivo

Para verificar se o dispositivo foi detectado corretamente, conclua as seguintes etapas:

1. Em um navegador da Web, faça logon no Insight RS Console.
2. No menu principal, selecione **Dispositivos** e clique na guia **Resumo do dispositivo**.

3. Verifique se a coluna Status contém um ícone de êxito ( ).

   Se não houver ícone de êxito, tente descobrir que coluna está com problema e consulte a Ajuda on-line para informações de solução de problemas.

# Capítulo 18: Configurar servidores Dell PowerEdge

Insight Remote Support (RS) deve ser capaz de se comunicar com o servidor Dell PowerEdge para que ele possa ser monitorado. Insight RS pode se comunicar com servidores Dell PowerEdge via SNMP. As informações a seguir descrevem como instalar e configurar os protocolos de comunicação e outros componentes de software recomendados, de modo que possam ser monitorados pelo Insight RS.

**Observação:** Insight RS oferece suporte aos sistemas operacionais Microsoft Windows Server 2008 e 2008 R2 para servidores Dell PowerEdge.

**Importante:** Não há suporte para coletas de configuração.

**Observação:** Se você tiver um controlador RAID instalado no seu sistema e planejar instalar a função de gerenciamento de armazenamento, assegure-se de que os drivers de dispositivo para cada controlador RAID também estejam instalados.

## Atender aos requisitos de configuração

Para configurar servidores Dell PowerEdge de forma que eles sejam monitorados pelo Insight RS, conclua as seguintes seções:

**Tabela 18.1** ***Etapas de configuração do servidor Dell PowerEdge***

| Tarefa | Concluída? |
|---|---|
| Certifique-se de que o Insight RS suporte seu servidor Dell PowerEdge, verificando o *Notas de Lançamento do HP Insight Remote Support*. | |
| Configurar o serviço SNMP do Windows no servidor Dell PowerEdge. | |
| Instale o Administrador do servidor Dell OpenManage no servidor Dell PowerEdge. | |
| Configure o destino da interceptação SNMP e a cadeia de caracteres da comunidade de leitura SNMP. | |
| Adicione o protocolo SNMP ao Insight RS Console. | |
| Detecte o servidor Dell PowerEdge no Insight RS Console. | |
| Adicione o Tipo de suporte e o Identificador de suporte do dispositivo ao Insight RS Console. | |

## Instalar e configurar o software de comunicação em servidores

Para configurar seus dispositivos monitorados, conclua as seguintes seções:

# Configurar o serviço SNMP do Windows

1. No dispositivo monitorado, abra a janela Propriedades do serviço SNMP e selecione a guia **Interceptações**.

2. No campo **Nome da comunidade**, digite o nome da comunidade SNMP e clique em **Adicionar à lista**.

**Importante:** O nome da comunidade deve corresponder ao nome da comunidade configurado no Console do Insight RS.

3. No campo destinos das interceptações, adicione o dispositivo host à lista:
   a. Para abrir a janela Configuração do serviço SNMP, clique em **Adicionar**.
   b. Digite o nome de host ou o endereço IP do dispositivo host.
   c. Clique em **Adicionar**.
4. Clique na guia **Segurança** e verifique se o nome da comunidade foi adicionado à lista de nomes de comunidades Aceitos.

5. Marque a caixa de seleção **Enviar interceptação de autenticação**.
6. Clique em **Aceitar pacotes SNMP de qualquer host**.
7. Clique em **OK** para salvar as configurações.

# Instalar e configurar o SNMP

O Administrador do servidor Dell OpenManage deve estar instalado no servidor Dell PowerEdge, e o serviço SNMP deve estar configurado.

Em servidores Windows 2008 e 2008 R2, a solução foi testada com o Administrador de servidor Dell OpenManage versão 6.2.0.

 **Importante:** Insight RS apenas oferece suporte à versão 6.2.0 do agente.

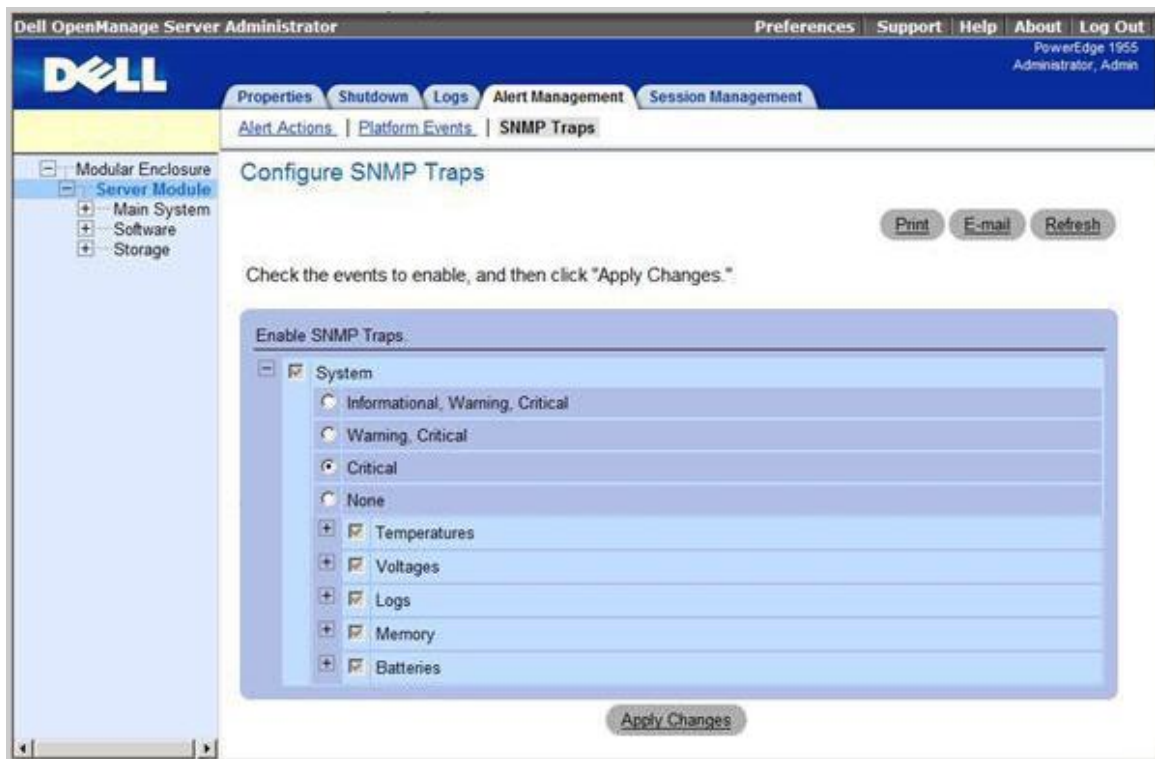
## *Instalar o Administrador de servidor Dell OpenManage*

Baixe e instale o Administrador de servidor Dell OpenManage. Para baixar esse software, acesse: http://content.dell.com/us/en/enterprise/d/solutions/openmanage-server-administrator.

**Observação:** Você pode verificar o driver do dispositivo no Windows, clicando com o botão direito em **My Computer** (Meu computador), selecionando **Manage** (Gerenciar) e em **Device Manager** (Gerenciador de dispositivos).

Veja também *Guia do usuário para instalação e segurança do Dell OpenManage*.

## *Configurar as armadilhas de SNMP no Administrador de servidor Dell OpenManage*

1. Abra o Administrador de servidor Dell OpenManage.
2. Clique na guia **Gerenciamento de alertas**.
3. Clique no link **Configuração SNMP**.
4. Selecione estas opções:
   - Sistema
   - Crítico
   - Temperaturas
   - Tensões
   - Logs
   - Memória
   - Baterias

5. Clique em **Aplicar alterações**.

# Adicionar credenciais de protocolo e iniciar a detecção

Para detectar seus dispositivos monitorados, conclua as seguintes seções:

## Criar uma credencial de protocolo SNMPv1 no Insight RS Console

Se a cadeia da comunidade SNMPv1 do dispositivo estiver definida como `pública` e o modo de acesso da comunidade for `somente leitura`, o Insight RS associará automaticamente um protocolo SNMP ao seu dispositivo. Se você usar uma cadeia de comunidade diferente ou uma porta não padrão, precisará criar uma credencial de protocolo SNMPv1 no Insight RS Console.

Para configurar o SNMPv1 no Insight RS Console, conclua as seguintes etapas:

1. Em um navegador da Web, faça logon no Insight RS Console.
2. No menu principal, selecione **Detecção** e clique na guia **Credenciais**.
3. Na lista suspensa Selecionar e configurar protocolo, selecione **Simple Network Management Protocol versão 1 (SNMPv1)**.
4. Clique em **Novo**. A caixa de diálogo Nova credencial é exibida.

5. Digite a cadeia de caracteres da comunidade configurada no seu dispositivo.
6. Clique em **Adicionar**.

O Insight RS cria a credencial de protocolo, que é exibida na tabela de credenciais.

# Detectar o dispositivo no Insight RS Console

Para detectar o dispositivo por meio do Insight RS Console, conclua as seguintes etapas:

1. Em um navegador da Web, faça logon no Insight RS Console.
2. No menu principal, selecione **Detecção** e clique na guia **Fontes**.
3. Expanda a seção Endereços IP e adicione o endereço IP do seu dispositivo:
   a. Clique em **Novo**.
   b. Selecione **Endereço único**, **Intervalo de endereços** ou **Lista de endereços**.
   c. Digite os endereços IP dos dispositivos a serem detectados.
   d. Clique em **Adicionar**.
4. Clique em **Iniciar detecção**.

# Configurar informações de garantia e contrato

Monitorar o suporte para servidores que não sejam da HP requer atenção especial aos dados de garantia e contrato do servidor. Os números de série e de produto que são detectados geralmente não combinam com os números de série e de produto listados no contrato de suporte HP.

Para digitar os números de série e de produto, siga estas instruções:

1. No Insight RS Console, verifique se o servidor é exibido na página Dispositivos.

**Importante:** Para o chassis do Dell PowerEdge, a coluna Produto fica vazia, por padrão.

2. Clique no **Nome do dispositivo** e, na guia **Dispositivo**, digite as seguintes informações:

**Observação:** A equipe de suporte de conta da HP deve configurar os dados de benefícios e para servidores Dell Windows no Insight RS Console.

- Número de série substituto (como listado no contrato)
- Número de produto substituto (como listado no contrato)
- Tipo de suporte
- Identificador de suporte

# Verificar o status de detecção e do dispositivo

Para verificar se o dispositivo foi detectado corretamente, conclua as seguintes etapas:

1. Em um navegador da Web, faça logon no Insight RS Console.
2. No menu principal, selecione **Dispositivos** e clique na guia **Resumo do dispositivo**.
3. Verifique se a coluna Status contém um ícone de êxito ( ).

   Se não houver ícone de êxito, tente descobrir que coluna está com problema e consulte a Ajuda on-line para informações de solução de problemas.

# Capítulo 19: Configurar gabinetes BladeSystem classe C

Os gabinetes HP BladeSystem classe C podem ser monitorados pelo Insight Remote Support (RS). Configurar o gabinete BladeSystem classe C somente permite que o Insight RS monitore o gabinete propriamente dito. Os blades instalados no gabinete BladeSystem classe C precisam ser configurados separadamente para serem monitorados pelo Insight RS. Consulte "Identificar componentes de software e protocolos de comunicação necessários", para obter informações sobre como configurar tipos de blades individuais.

Configure gabinetes BladeSystem classe C usando um dos dois métodos, dependendo da versão do firmware do Onboard Administrator (OA) que você está usando:

 **Importante:** Não tente usar os dois métodos de configuração no mesmo dispositivo host.

- Versão de firmware do OA 3.60 ou superior, registre o Insight Remote Support por meio do OA.

  Consulte "Registrar o Remote Support via Onboard Administrator".

  Se você estiver usando um OA primário e em standby, assegure-se de que a versão do firmware para ambos os OAs é a 3.60 ou superior.
- Versão de firmware do OA anterior à 3.55, configure o Insight Remote Support usando SNMP.

  Consulte "Configurar o SNMP no gabinete BladeSystem classe C".

  Se você estiver usando um OA primário e em standby, limite a detecção a um dos OAs, não a ambos.

Se estiver usando as versões de firmware 3.55 ou 3.56 do OA, a HP recomenda que você atualize para a versão 3.60.

## Configurar gabinetes BladeSystem classe C com o OA

Os gabinetes HP BladeSystem classe C podem ser monitorados pelo Insight Remote Support (RS). Configurar o gabinete BladeSystem classe C somente permite que o Insight RS monitore o gabinete propriamente dito. Os blades instalados no gabinete BladeSystem classe C precisam ser configurados separadamente para serem monitorados pelo Insight RS. Consulte "Identificar componentes de software e protocolos de comunicação necessários", para obter informações sobre como configurar tipos de blades individuais.

Os gabinetes BladeSystem classe C podem ser monitorados com o uso dos recursos de gerenciamento incorporados no OA ou com a configuração do SNMP no OA, dependendo do nível de firmware do OA:

**Importante:** ***Não*** tente configurar ambos os métodos de configuração. Não há suporte para essa estratégia, e o monitoramento não funcionará corretamente.

1. Nível de firmware do OA **3.60 ou superior**: Registre-se com um dispositivo host do Insight Remote Support 7.4 por meio do OA para enviar eventos de serviço ao dispositivo host referentes ao OA primário e ao OA em espera.

**Importante:** Para solucionar vulnerabilidades de softwares de terceiros, a HP recomenda o uso do OA 4.30 ou versão posterior. Para acessar a interface Web do OA 4.30 ou versão posterior, você deve habilitar o TLS no seu navegador. O TLS é o sucessor do SSL (Secure Sockets Layer).

2. Nível de firmware do OA **anterior à versão 3.55**: Se você tiver configurado um OA primário e um OA em espera no seu ambiente, será necessário configurar o protocolo **SNMP** para enviar interceptações ao dispositivo host. A detecção feita no dispositivo host do Insight Remote Support deve se limitar a apenas um dos OAs. Se você estiver usando uma versão de firmware anterior à versão 3.55, consulte "Configurar gabinetes BladeSystem classe C usando SNMP".

   **Observação:** Se estiver usando as versões de firmware 3.55 ou 3.56 do OA, a HP recomenda que você atualize para a versão 3.60.

O software do firmware mais atual pode ser encontrado no website da HP em: www.hp.com/support/oa.

# Atender aos requisitos de configuração

Para configurar gabinetes BladeSystem classe C via OA de forma que eles sejam monitorados pelo Insight RS, conclua as seguintes seções:

**Tabela 19.1** ***Etapas de configuração de gabinetes BladeSystem classe C usando o OA***

| Tarefa | Concluída? |
| --- | --- |
| Verifique se o Insight RS ofereça suporte ao seu gabinete BladeSystem classe C, consultando as *Notas de Lançamento do HP Insight Remote Support*. | |
| Registrar o Remote Support através do Administrador Incorporado. | |
| Verifique o status do gabinete BladeSystem classe C no Insight RS Console. | |
| Envie um evento de teste para verificar a conectividade entre seu gabinete BladeSystem classe C e o Insight RS. | |

# Configurar dispositivos monitorados

Para configurar seus dispositivos monitorados, conclua a seguinte seção:

## *Definir configurações de firewall e porta*

Para obter uma lista completa de requisitos de firewall e de porta para dispositivos monitorados, consulte o *Informe de Segurança do HP Insight Remote Support*, em: http://www.hp.com/go/insightremotesupport/docs.

# Registrar o OA e verificar a detecção

Para detectar seus dispositivos monitorados, conclua as seguintes seções:

## *Registrar o Remote Support via Onboard Administrator*

Se você estiver usando a versão de firmware 3.60 ou superior do OA, poderá habilitar o Insight Remote Support para um gabinete BladeSystem classe C usando o Onboard Administrator (OA). O OA não é responsável por relatar informações sobre os blades instalados nos gabinetes BladeSystem classe C. O

OA só relata problemas de gabinetes, como problemas com ventoinhas, fontes de alimentação e compartimentos de mídia.

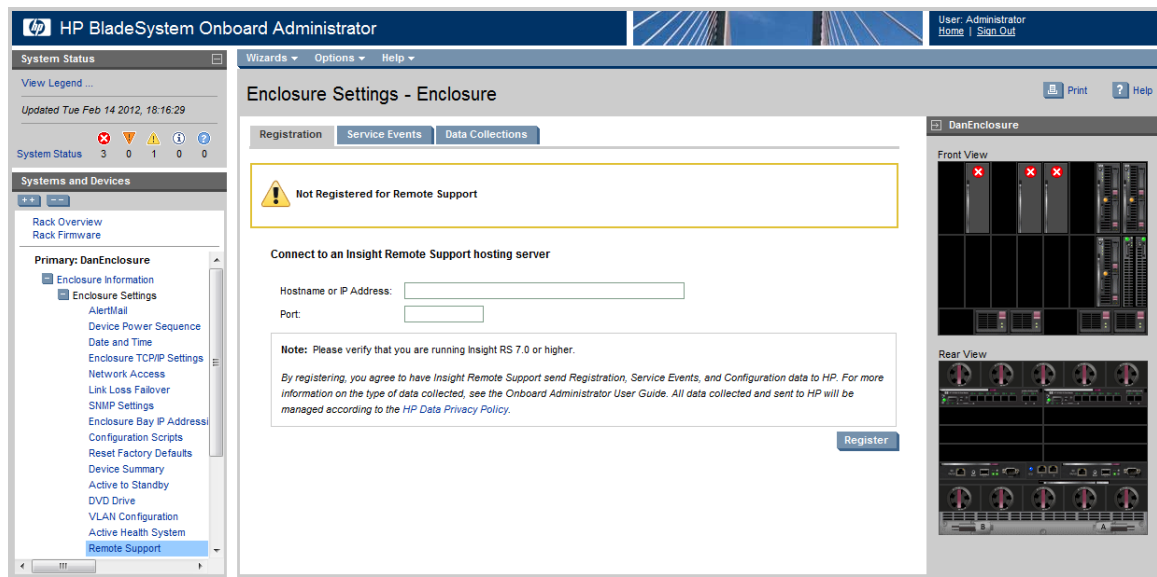
**Importante:** Para solucionar vulnerabilidades de softwares de terceiros, a HP recomenda o uso do iLO 4 2.03 ou versão posterior. Para acessar a interface Web do iLO 4 2.03 ou versão posterior, você deve habilitar o TLS no seu navegador. O TLS é o sucessor do SSL (Secure Sockets Layer).

**Importante:** Se você estiver usando um OA primário e em standby, assegure-se de que a versão do firmware para ambos os OAs é a 3.60 ou superior.

**Importante:** Ao se registrar-se para o Remote Support via OA, certifique-se de que seu destino de interceptação esteja definido como o mesmo dispositivo host do Insight RS registrado para o Remote Support. Quando o OA envia eventos de serviço ao dispositivo host, ele também gera interceptações SNMP que são enviadas ao destino de interceptação SNMP. O destino de interceptação SNMP precisa ser o mesmo dispositivo host do Insight RS; caso contrário, eventos duplicados serão relatados para a HP.

Registrar o gabinete não registra os blades individuais instalados no gabinete. É preciso configurar cada blade separadamente.

Para se registrar para o Remote Support através do OA, siga estas instruções:

1. Em um navegador da Web, faça login no Administrador Incorporado do HP BladeSystem (`https://`*<nome de host ou endereço IP do OA>*).
2. Navegue até **Informações do gabinete** → **Configurações do gabinete** → **Acesso à rede** e clique na guia **Protocolos**.
3. Certifique-se de que a caixa de seleção **Habilitar resposta XML** esteja marcada. Se essa caixa de seleção não estiver marcada, o OA não poderá ser habilitado no Insight RS.
4. Navegue até **Informações do gabinete** → **Configurações do gabinete** → **Remote Support** e clique na guia **Registro**.

5. Digite o nome de host ou endereço IP.
6. No campo **Porta**, digite *7906*.
7. Clique em **Registrar**.

## *Verificar o status de detecção e do dispositivo*

Para verificar se o dispositivo foi detectado corretamente, conclua as seguintes etapas:

1. Em um navegador da Web, faça logon no Insight RS Console.
2. No menu principal, selecione **Dispositivos** e clique na guia **Resumo do dispositivo**.
3. Verifique se a coluna Status contém um ícone de êxito ( ).

   Se não houver ícone de êxito, tente descobrir que coluna está com problema e consulte a Ajuda on-line para informações de solução de problemas.

# Verificar a comunicação entre o dispositivo monitorado e o Insight RS

Para verificar a comunicação entre o dispositivo monitorado e o Insight RS, conclua as seguintes seções:

## *Enviar um evento de teste*

Depois de registrar o gabinete classe C no Insight Remote Support, envie um evento de teste para confirmar a conexão.

1. No menu de navegação do OA, clique em **Configurações do gabinete** → **Remote Support** → **Eventos de serviço**. Aparece a tela Eventos de serviço.
2. Clique em **Enviar evento de teste**.

   Quando a transmissão estiver concluída, o evento de teste será listado no Log de eventos de serviço e no Insight RS Console.

A coluna Hora de criação, no Log de eventos de serviço, mostra a data e a hora com base no fuso horário do gabinete configurado.

3. Confira o Insight RS Console para verificar se o evento de teste chegou:
   a. Faça logon no Insight RS Console.
   b. No Menu principal, selecione **Dispositivos**.
   c. Localize o gabinete classe C e clique no nome do dispositivo.
   d. Clique na guia **Eventos de serviços**. Todos os eventos de serviço enviados sobre o sistema são exibidos aqui (mesmo se você limpar o Log de eventos de serviço).

      O Insight RS converte o valor de hora de geração do evento de serviço do OA no fuso horário do navegador usado para acessar o Insight RS Console.

**Observação:** Os eventos de teste são automaticamente fechados pela HP, já que nenhuma ação mais é necessária.

## *Verificar coletas no Insight RS Console*

Coletas não são executadas automaticamente depois da descoberta. A HP recomenda que você execute uma coleta manualmente após a descoberta completa para verificar a conectividade. Execute o cronograma de coleta manualmente na guia Serviços de coleta → Agendamentos de coleta. Para obter mais informações sobre o agendamento de coletas, consulte a Ajuda do Insight RS.

Verifique se essa coleta foi bem-sucedida na guia Serviços de coleta → Resultados da coleta básica do Insight RS Console.

1. Faça logon no Insight RS Console.
2. No menu principal, selecione **Serviços de coleta** e depois clique na guia **Resultados da coleta básica**.
3. Expanda a seção Coleta de configurações básicas do servidor.
4. Localize a entrada referente ao seu dispositivo e verifique a coluna Resultado. Se a coleta tiver sido bem-sucedida, um ícone de êxito será exibido (). Se ocorrer uma falha, um ícone de erro será exibido ().

# Manutenção e solução de problemas

## *Desativar o monitoramento de um gabinete BladeSystem classe C*

Pode haver um motivo para você precisar desabilitar temporariamente um gabinete BladeSystem classe C que não é mais reconhecido pelo Insight Remote Support. Por exemplo, para manutenção de rotina do dispositivo ou se a garantia do gabinete tiver vencido.

**Importante:** Desabilitar o gabinete classe C no Insight RS Console não cancela o registro do dispositivo no OA. Para o OA saber que o dispositivo foi desabilitado, você deve cancelar o registro no OA em vez de desabilitar o dispositivo no Insight RS Console.

Observe o seguinte:

- Desabilitar ou excluir o gabinete classe C no Insight RS Console não cancela o registro do dispositivo no OA. Para o OA saber que o gabinete foi desabilitado, você deve usar o OA para cancelar o registro no Insight Remote Support. Além disso, se o gabinete for excluído no Insight RS Console e o OA enviar uma interceptação SNMP, o Insight RS acionará uma nova detecção do gabinete e provavelmente reabilitará o dispositivo para suporte remoto.
- Cancelar o registro de um gabinete no OA interrompe temporariamente o monitoramento desse gabinete, mas ele ainda fica listado no Insight RS Console. Para retomar o monitoramento, use o software OA, para registrar novamente o gabinete.

Para cancelar temporariamente o registro do Insight RS, conclua as seguintes etapas:

1. Em um navegador da Web, faça login no Administrador Incorporado do HP BladeSystem (`https://`*`<nome de host ou endereço IP do OA>`*).
2. Navegue até **Informações do gabinete** → **Configurações do gabinete** → **Remote Support**.
3. Clique em **Cancelar registro**. A seguinte mensagem aparece:

   `Você tem certeza de que deseja cancelar o registro e desabilitar o HP Insight Remote Support?`
4. Clique em **OK**. A seguinte mensagem aparece:

   `Cancelamento de registro em andamento. Aguarde...`

   Quando o cancelamento de registro for concluído, a página do Remote Support mostrará a seguinte mensagem:

   `O gabinete não está registrado.`

O sistema desabilitará o monitoramento e as coletas no dispositivo.

# Configurar gabinetes BladeSystem classe C usando SNMP

Os gabinetes HP BladeSystem classe C podem ser monitorados pelo Insight Remote Support (RS). Configurar o gabinete BladeSystem classe C somente permite que o Insight RS monitore o gabinete propriamente dito. Os blades instalados no gabinete BladeSystem classe C precisam ser configurados separadamente para serem monitorados pelo Insight RS. Consulte "Identificar componentes de software e protocolos de comunicação necessários", para obter informações sobre como configurar tipos de blades individuais.

Se você estiver usando a versão 3.60 ou superior, a HP recomenda registrar o seu gabinete classe C com o OA. Para obter mais informações, consulte "Configurar gabinetes BladeSystem classe C com o OA". Se estiver usando as versões de firmware 3.55 ou 3.56 do OA, a HP recomenda que você atualize para a versão 3.60.

# Atender aos requisitos de configuração

Para configurar gabinetes BladeSystem classe C usando o SNMP de forma que eles sejam monitorados pelo Insight RS, conclua as seguintes seções:

**Tabela 19.2** ***Etapas de configuração do gabinete BladeSystem classe C usando o SNMP***

| Tarefa | Concluída? |
|---|---|
| Verifique se o Insight RS ofereça suporte ao seu gabinete BladeSystem classe C, consultando as *Notas de Lançamento do HP Insight Remote Support*. | |
| Configure o SNMP no gabinete BladeSystem classe C. | |
| Adicione o protocolo SNMP ao Insight RS Console. | |
| Detecte o gabinete BladeSystem classe C no Insight RS Console. | |
| Envie um evento de teste para verificar a conectividade entre seu gabinete BladeSystem classe C e o Insight RS. | |

# Instalar e configurar o software de comunicação em gabinetes

Para configurar seus dispositivos monitorados, conclua as seguintes seções:

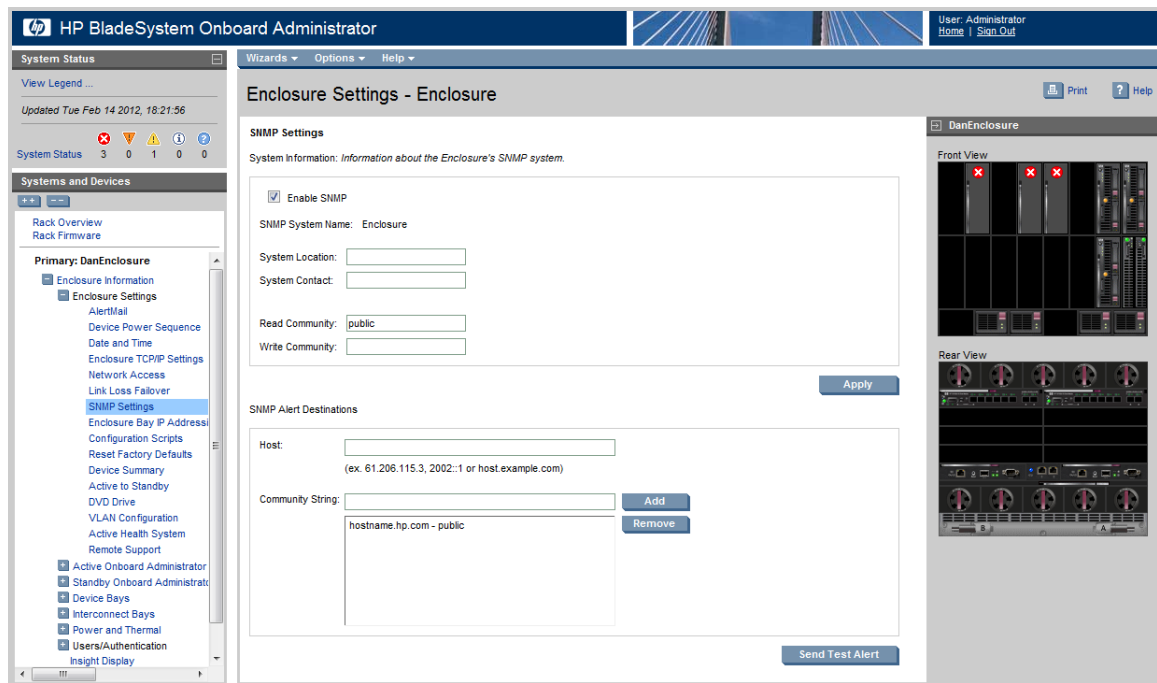
## *Configurar o SNMP no gabinete BladeSystem classe C*

Se você estiver usando uma versão do firmware anterior à 3.55, precisará configurar o SNMP no Administrador Incorporado (OA) antes de o gabinete poder ser monitorado pelo Insight RS.

Configurar o gabinete para o Remote Support não permite que o Insight RS monitore os blades instalados no gabinete. É preciso configurar cada blade separadamente.

**Importante:** Se você estiver usando um OA primário e em standby, limite a detecção a um dos OAs, não a ambos.

Para configurar o SNMP, conclua as seguintes etapas:

1. Em um navegador da web, abra o Administrador Incorporado do HP BladeSystem.
2. Na tela de login, digite o nome de usuário e a senha e clique em **Entrar**.
3. Expanda **Informações sobre o gabinete** → **Configurações do gabinete**.
4. Clique em **Configurações de SNMP**.

5. No painel Informações do sistema, marque a caixa de seleção **Habilitar SNMP** e conclua as seguintes etapas:
   a. Acrescente a localização do sistema e as informações de contato.
   b. Defina as cadeias de caracteres de comunidade de leitura e gravação.
   c. Clique em **Aplicar**.
6. Na página Destinos de alerta SNMP, conclua as seguintes etapas:
   a. No campo **Host**, digite o endereço de IP do dispositivo host.
   b. No campo **Cadeia de caracteres de comunidade**, digite a cadeia de caracteres de comunidade SNMP para o dispositivo host.
   c. Clique em **Adicionar**.

## Definir configurações de firewall e porta

Para obter uma lista completa de requisitos de firewall e de porta para dispositivos monitorados, consulte o *Informe de Segurança do HP Insight Remote Support*, em: http://www.hp.com/go/insightremotesupport/docs.

# Adicionar credenciais de protocolo e iniciar a detecção

Para detectar seus dispositivos monitorados, conclua as seguintes seções:

## Criar uma credencial de protocolo SNMPv1 no Insight RS Console

Se a cadeia da comunidade SNMPv1 do dispositivo estiver definida como `pública` e o modo de acesso da comunidade for `somente leitura`, o Insight RS associará automaticamente um protocolo SNMP ao seu dispositivo. Se você usar uma cadeia de comunidade diferente ou uma porta não padrão, precisará criar uma credencial de protocolo SNMPv1 no Insight RS Console.

Para configurar o SNMPv1 no Insight RS Console, conclua as seguintes etapas:

1. Em um navegador da Web, faça logon no Insight RS Console.
2. No menu principal, selecione **Detecção** e clique na guia **Credenciais**.
3. Na lista suspensa Selecionar e configurar protocolo, selecione **Simple Network Management Protocol versão 1 (SNMPv1)**.
4. Clique em **Novo**. A caixa de diálogo Nova credencial é exibida.
5. Digite a cadeia de caracteres da comunidade configurada no seu dispositivo.
6. Clique em **Adicionar**.

O Insight RS cria a credencial de protocolo, que é exibida na tabela de credenciais.

### Detectar o dispositivo no Insight RS Console

**Observação:** Se houver um problema com a comunicação HTTPS (SSL), a descoberta tentará usar HTTP para descobrir o dispositivo.

Para detectar o dispositivo por meio do Insight RS Console, conclua as seguintes etapas:

1. Em um navegador da Web, faça logon no Insight RS Console.
2. No menu principal, selecione **Detecção** e clique na guia **Fontes**.
3. Expanda a seção Endereços IP e adicione o endereço IP do seu dispositivo:
   a. Clique em **Novo**.
   b. Selecione **Endereço único**, **Intervalo de endereços** ou **Lista de endereços**.
   c. Digite os endereços IP dos dispositivos a serem detectados.
   d. Clique em **Adicionar**.
4. Clique em **Iniciar detecção**.

### Verificar o status de detecção e do dispositivo

Para verificar se o dispositivo foi detectado corretamente, conclua as seguintes etapas:

1. Em um navegador da Web, faça logon no Insight RS Console.
2. No menu principal, selecione **Dispositivos** e clique na guia **Resumo do dispositivo**.
3. Verifique se a coluna Status contém um ícone de êxito ( ).

   Se não houver ícone de êxito, tente descobrir que coluna está com problema e consulte a Ajuda on-line para informações de solução de problemas.

## Verificar a comunicação entre o dispositivo monitorado e o Insight RS

Para verificar a comunicação entre o dispositivo monitorado e o Insight RS, conclua as seguintes seções:

### Verificar o monitoramento de eventos de serviço

Para enviar um evento de teste, siga estas etapas:

1. Em um navegador da web, abra o Administrador Incorporado do HP BladeSystem.
2. Na tela de login, digite o nome de usuário e a senha e clique em **Entrar**.
3. Expanda **Informações sobre o gabinete** → **Configurações do gabinete**.
4. Clique em **Configurações de SNMP**.
5. Clique em **Enviar alerta de teste** para enviar um teste de armadilha SNMP ao dispositivo host.

### Verificar coletas no Insight RS Console

Coletas não são executadas automaticamente depois da descoberta. A HP recomenda que você execute uma coleta manualmente após a descoberta completa para verificar a conectividade. Execute o cronograma de coleta manualmente na guia Serviços de coleta → Agendamentos de coleta. Para obter mais informações sobre o agendamento de coletas, consulte a Ajuda do Insight RS.

Verifique se essa coleta foi bem-sucedida na guia Serviços de coleta → Resultados da coleta básica do Insight RS Console.

1. Faça logon no Insight RS Console.
2. No menu principal, selecione **Serviços de coleta** e depois clique na guia **Resultados da coleta básica**.
3. Expanda a seção Coleta de configurações básicas do servidor.
4. Localize a entrada referente ao seu dispositivo e verifique a coluna Resultado. Se a coleta tiver sido bem-sucedida, um ícone de êxito será exibido (). Se ocorrer uma falha, um ícone de erro será exibido ().

## Manutenção e solução de problemas

### Desativar o monitoramento de um gabinete BladeSystem classe C

Pode haver um motivo para você precisar desabilitar temporariamente um gabinete BladeSystem classe C que não é mais reconhecido pelo Insight Remote Support. Por exemplo, para manutenção de rotina do dispositivo ou se a garantia do gabinete tiver vencido.

Para desabilitar um dispositivo no Insight Remote Support, conclua as seguintes etapas:

1. No Menu principal, selecione **Dispositivos**.
2. Clique na guia **Resumo do dispositivo**.
3. Na coluna mais à esquerda, marque a caixa de seleção dos dispositivos que você deseja desabilitar.
4. Clique em **Ações** → **Desabilitar selecionados** e em **OK** na caixa de diálogo de confirmação.

O sistema desabilitará o monitoramento e as coletas no dispositivo.

# Configurar módulos Virtual Connect

Módulos HP Virtual Connect exigem o SNMP para monitoramento e coletas de eventos.

# Atender aos requisitos de configuração

Para configurar Módulos Virtual Connect de forma que eles sejam monitorados pelo Insight RS, conclua as seguintes seções:

**Tabela 19.3** ***Etapas de configuração de módulos Virtual Connect***

| Tarefa | Concluída? |
|---|---|
| Certifique-se de que o Insight RS ofereça suporte ao módulo Virtual Connect, verificando o *Notas de Lançamento do HP Insight Remote Support*. | |
| Configure o SNMP no HP Virtual Connect Manager que gerencia os seus Módulos Virtual Connect. | |
| Adicione o protocolo SNMP ao Insight RS Console. | |
| Detecte o Módulo Virtual Connect no Insight RS Console. | |

# Configurar o software de comunicação em Módulos Virtual Connect

Para configurar seus dispositivos monitorados, conclua as seguintes seções:

## *Configurar o SNMP no Módulo Virtual Connect*

Para configurar o SNMP, conclua as seguintes etapas:

1. Em um navegador da Web, abra o HP Virtual Connect Manager que gerencia os seus Módulos Virtual Connect.
2. Na tela de login, digite o nome de usuário e a senha e clique em **Entrar**.
3. No menu esquerdo, clique em Configuração SNMP na seção Configuração do domínio.
4. Na guia Configurações, na seção Configuração SNMP, habilite o SNMP:
   a. Marque a caixa de seleção **Habilitar SNMP V1/V2** para módulos Ethernet e módulos FlexFabric.
   b. Marque a caixa de seleção **Habilitar SNMP V1/V2** para módulos Fibre Channel.

5. Na seção Destinos de interceptações SNMP, adicione o destino de interceptação para o dispositivo host do Insight RS.
6. Clique em **Aplicar**.

## *Definir configurações de firewall e porta*

Para obter uma lista completa de requisitos de firewall e de porta para dispositivos monitorados, consulte o *Informe de Segurança do HP Insight Remote Support*, em: http://www.hp.com/go/insightremotesupport/docs.

# Adicionar credenciais de protocolo e iniciar a detecção

Para detectar seus dispositivos monitorados, conclua as seguintes seções:

## *Criar uma credencial de protocolo SNMP no Insight RS Console*

Se a cadeia da comunidade SNMPv1 do dispositivo estiver definida como `pública` e o modo de acesso da comunidade for `somente leitura`, o Insight RS associará automaticamente um protocolo SNMP ao seu dispositivo. Se você usar uma cadeia de comunidade diferente ou uma porta não padrão, precisará criar uma credencial de protocolo SNMP no Insight RS Console.

Para configurar o SNMP no Insight RS Console, conclua as seguintes etapas:

1. Em um navegador da Web, faça logon no Insight RS Console.
2. No menu principal, selecione **Detecção** e clique na guia **Credenciais**.
3. Na lista suspensa Selecionar e configurar protocolo, selecione **Simple Network Management Protocol versão 1 (SNMPv1)** ou **Simple Network Management Protocol versão 2 (SNMPv2)**.
4. Clique em **Novo**. A caixa de diálogo Nova credencial é exibida.
5. Digite a cadeia de caracteres da comunidade configurada no seu dispositivo.
6. Clique em **Adicionar**.

O Insight RS cria a credencial de protocolo, que é exibida na tabela de credenciais.

### Detectar o dispositivo no Insight RS Console

Para detectar o dispositivo por meio do Insight RS Console, conclua as seguintes etapas:

1. Em um navegador da Web, faça logon no Insight RS Console.
2. No menu principal, selecione **Detecção** e clique na guia **Fontes**.
3. Expanda a seção Endereços IP e adicione o endereço IP do seu dispositivo:
   a. Clique em **Novo**.
   b. Selecione **Endereço único**, **Intervalo de endereços** ou **Lista de endereços**.
   c. Digite os endereços IP dos dispositivos a serem detectados.
   d. Clique em **Adicionar**.
4. Clique em **Iniciar detecção**.

### Verificar o status de detecção e do dispositivo

Para verificar se o dispositivo foi detectado corretamente, conclua as seguintes etapas:

1. Em um navegador da Web, faça logon no Insight RS Console.
2. No menu principal, selecione **Dispositivos** e clique na guia **Resumo do dispositivo**.
3. Verifique se a coluna Status contém um ícone de êxito ().

   Se não houver ícone de êxito, tente descobrir que coluna está com problema e consulte a Ajuda on-line para informações de solução de problemas.

## Verificar a comunicação entre o dispositivo monitorado e o Insight RS

Para verificar a comunicação entre o dispositivo monitorado e o Insight RS, conclua as seguintes seções:

### Verificar coletas no Insight RS Console

Coletas não são executadas automaticamente depois da descoberta. A HP recomenda que você execute uma coleta manualmente após a descoberta completa para verificar a conectividade. Execute o cronograma de coleta manualmente na guia Serviços de coleta → Agendamentos de coleta. Para obter mais informações sobre o agendamento de coletas, consulte a Ajuda do Insight RS.

Verifique se essa coleta foi bem-sucedida na guia Serviços de coleta → Resultados da coleta básica do Insight RS Console.

1. Faça logon no Insight RS Console.
2. No menu principal, selecione **Serviços de coleta** e depois clique na guia **Resultados da coleta básica**.
3. Expanda a seção Coleta de configurações básicas do servidor.
4. Localize a entrada referente ao seu dispositivo e verifique a coluna Resultado. Se a coleta tiver sido bem-sucedida, um ícone de êxito será exibido ( ). Se ocorrer uma falha, um ícone de erro será exibido ( ).

# Capítulo 20: Configurar Enterprise Virtual Arrays e P6000

O servidor P6000 Command View pode ser um servidor independente com software Command View e SMIS-S instalados (chamados de Gerenciamento baseado em servidor - SBM) ou pode ser incorporado ao dispositivo EVA em si, chamado de Gerenciamento baseado em matriz - ABC.

- Para configurar um P6000 ou EVA usando o Gerenciamento baseado em servidor, consulte "Configurar Enterprise Virtual Arrays e P6000 com o gerenciamento baseado em servidor"
- Para configurar um P6000 ou EVA usando o Gerenciamento baseado em matriz, consulte "Configurar Enterprise Virtual Arrays e P6000 com o gerenciamento baseado em array"

## Configurar Enterprise Virtual Arrays e P6000 com o gerenciamento baseado em servidor

As informações abaixo se aplicam a ambos os dispositivos monitorados e host que hospedam o P6000 Command View. O sistema ProLiant Windows hospedando o P6000 Command View tem os mesmos requisitos e configurações de sistema de qualquer servidor ProLiant Windows (consulte "Configurar servidores ProLiant Windows"). Certifique-se de definir suas credenciais WMI e/ou SNMP corretamente. Além disso, você deve instalar o Coletor de monitoramento do log de eventos (ELMC) no dispositivo monitorado.

Antes de instalar e configurar o Insight Remote Support:

1. Verifique se o P6000 Command View 9.4 ou superior está instalado no dispositivo host.

   Acesse o Painel de controle do Windows e verifique se o HP P6000 Command View aparece na janela Add/Remove Programs (Adicionar/Remover programas).
2. Verifique se os componentes SMI-S EVA e SMI-S CIMOM (os dois componentes que compõem o SMI-S) estão instalados no dispositivo host.

   Confirme se o componente está instalado e em execução verificando a presença e o status do serviço `HP CIM Object Manager`.

**Observação: A HP recomenda enfaticamente que você ative o Adaptador de e-mail em Configurações do administrador** → guia Adaptadores de integração e que, no mínimo, selecione estas notificações: *Caso aberto*, *Falha do aplicativo*, *Vencimento do direito* e *Alteração do dispositivo*.

## Atender aos requisitos de configuração

Para configurar Enterprise Virtual Arrays e P6000 usando o SBM para que eles sejam monitorados pelo Insight RS, conclua as seguintes seções:

**Tabela 20.1** ***Etapas de configuração de Enterprise Virtual Arrays e P6000 usando o SBM***

| Tarefa | Concluída? |
|---|---|
| Certifique-se de que o Insight RS suporte sua matriz de discos P6000, verificando o *Notas de Lançamento do HP Insight Remote Support*. | |
| Verifique se o HP P6000 Command View está instalado e configurado no Servidor de gerenciamento de armazenamento. | |
| Instale o ELMC no Servidor de gerenciamento de armazenamento. | |
| Adicione o ELMC ao Insight RS Console. | |
| Adicione o P6000 Command View ao Insight RS Console. | |
| Detecte o P6000 no Insight RS Console. | |
| Verifique se as informações de garantia e de contrato do dispositivo no Insight RS Console. | |
| Envie um evento de teste para verificar a conectividade entre o seu P6000 e o Insight RS. | |

# Instalar e configurar o software de comunicação em arrays

Para configurar seus dispositivos monitorados, conclua as seguintes seções:

## *Instalar o HP P6000 Command View*

O Insight Remote Support e o software P6000 Command View têm suporte para coexistência no dispositivo host, desde que os requisitos mínimos de hardware e software sejam atendidos. A HP recomenda co-hospedar o software P6000 Command View no dispositivo host do Insight Remote Support. Ambientes com várias instâncias do P6000 Command View podem ter uma instância no dispositivo host e outras instâncias do P6000 Command View em outros dispositivos monitorados.

Várias instâncias do P6000 Command View podem compartilhar a função de gerenciamento de matrizes EVA anexas comuns no ambiente. Isso pode servir, por exemplo, ao propósito de tolerância a falhas ou ao equilíbrio de carga. Embora possa haver várias instâncias do P6000 Command View capazes de gerenciar a matriz EVA, apenas uma instância do P6000 Command View pode ser o gerenciador ativo daquela matriz. Outras instâncias do P6000 Command View que não estão ativas no gerenciamento da matriz são consideradas passivas.

**Observação:** Dados de evento em tempo real e comunicação para a matriz só são possíveis quando há uma conexão com a instância do P6000 Command View que é o gerenciador ativo da matriz. Para configurar um dispositivo monitorado, você deve instalar o ELMC em qualquer servidor que esteja executando o P6000 Command View, que seja capaz de ser o gerenciador ativo da matriz. Qualquer instância do P6000 Command View que não seja o gerenciador ativo de um EVA é considerada como uma instância passiva do P6000 Command View. Dados históricos do evento podem estar presentes em uma instância passiva se ela já tiver sido o gerenciador ativo. Esses dados de evento podem ser úteis para a análise manual.

**Importante:** Uma instância passiva do P6000 Command View pode ver a matriz, mas não pode se comunicar com ela. Apenas a instância gerenciadora ativa é capaz de se comunicar com a matriz. É por isso que é possível ver uma matriz detectada, mas falta informação sobre ela em alguns componentes.

Para ter suporte no Insight Remote Support, o dispositivo monitorado deve ter o P6000 Command View instalado (versão 9.4 ou posterior) e gerenciar pelo menos uma matriz. O SMI-S é fornecido com a instalação do P6000 Command View e é necessário porque funciona como via de comunicação entre o Insight Remote Support e a matriz, utilizando o CIMOM para comunicações WBEM.

Se os componentes do P6000 Command View necessários *não* estão instalados, consulte "Documentação do P6000 Command View", para mais detalhes.

---

**Cuidado:** Remover o SMI-S de um sistema host também força a remoção do Command View for Tape Libraries (TL). A versão do Command View TL deve corresponder ao firmware utilizado na biblioteca.

Se a versão do SMI-S instalado pelo Command View TL for anterior à usada pelo P6000 Command View, instale ou atualize o P6000 Command View *após* o Command View TL, para evitar um conflito.

Além disso, as credenciais usadas por cada aplicativo de software são substituídas pelo outro, ao ser instalado. Portanto, use a mesma conta para ambos.

---

### *Atender aos requisitos de sistema e acesso do P6000 Command View*

Requisitos de acesso:

- As versões suportadas do P6000 Command View usam um projeto de logon seguro (SSL).
- É necessária uma conta do Microsoft Windows, com o privilégio de grupo correto, para acessar o P6000 Command View.

Instalar o P6000 Command View adiciona dois novos privilégios de grupo a um sistema: HP Storage Admins (acesso de escrita) e HP Storage Users (acesso de leitura). Credenciais do P6000 Command View são necessárias ao configurar o Insight Remote Support. Portanto, verifique se você tem essas informações.

### *Instalar o HP SIM e o P6000 Command View no mesmo servidor*

### *Noções básicas dos conflitos de configuração de porta do HP SIM*

A atribuição padrão de porta de 5989 para WBEM/WMI e SMI-S gerou conflitos com o HP SIM no dispositivo host. A capacidade do Insight RS de fazer interface com indicações WBEM, o WMI Mapper e a inclusão de sistemas HP-UX no ambiente adicionam mais complexidade à configuração do ambiente. O uso da porta 5989 está embutido no HP-UX. As seções a seguir descrevem alterações que lidam com problemas de atribuição de portas e oferecem uma nova solução para a configuração do Insight Remote Support com o P6000 Command View.

---

**Observação:** Se o seu ambiente do Insight Remote Support já estiver configurado e operacional, você pode preferir deixar as configurações como estão e implementar as instruções a seguir apenas se tiver problemas relacionados.

---

A sequência de instalação do HP SIM e do P6000 Command View em um dispositivo host afeta as configurações padrão de portas. A prática recomendada é instalar o HP SIM primeiro e permitir que o WMI Mapper use a porta padrão 5989. A instalação subsquente do P6000 Command View pode detectar se a porta 5989 está sendo usada e, se for o caso, redirecionar para uma porta diferente.

Para obter um instantâneo das atribuições de porta atuais no seu ambiente, em uma janela de comando, execute o seguinte comando:

```
C:\ netstat –anb >netstat.txt
```

### *Instalar o HP SIM pela primeira vez*

Ao instalar o HP SIM pela primeira vez, o assistente inicial inclui uma etapa para configurar o Proxy do WBEM/WMI Mapper.

Mantenha a configuração padrão da porta 5989. Depois de concluir a instalação do HP SIM, adicione a porta que o P6000 Command View SMI-S usará para o arquivo `.xml` mostrado na etapa 1 do procedimento a seguir.

Siga essas etapas para identificar a porta que o HP SIM usará para se conectar ao SMI-S. Neste exemplo, a porta 60000 é usada para a conexão HTTPS do SMI-S com o namespace **interop**.

1. Abra o seguinte arquivo em um editor de texto:

   ```
   C:\Program Files\HP\Systems Insight Manager\config\identification\wbemportlist.xml
   ```

2. Adicione as seguintes linhas de texto em *vermelho* ao final do arquivo.

   ```
   <port id="60000" protocol="https">
     <interopnamespacelist>
       <interopnamespace name="interop"/>
     </interopnamespacelist>
   </port>
   ```

   O exemplo a seguir mostra o arquivo completo, depois que você adiciona a porta para o SMI-S:

   ```
   <?xml version="1.0" encoding="UTF-8"?>
   <wbemportlist>
     <port id="5989" protocol="https">
       <cimnamespacelist>
         <cimnamespace name="root/cimv2"/>
         <cimnamespace name="vmware/esxv2"/>
         <cimnamespace name="root/hpq"/>
       </cimnamespacelist>
       <interopnamespacelist>
         <interopnamespace name="root/pg_interop"/>
         <interopnamespace name="root"/>
         <interopnamespace name="root/emulex"/>
         <interopnamespace name="root/qlogic"/>
         <interopnamespace name="root/ibm"/>
         <interopnamespace name="root/emc"/>
         <interopnamespace name="root/smis/current"/>
   ```

```
        <interopnamespace name="root/hitachi/dm51"/>
        <interopnamespace name="interop"/>
        <interopnamespace name="root/interop"/>
        <interopnamespace name="root/switch"/>
        <interopnamespace name="root/cimv2"/>
      </interopnamespacelist>
    </port>
    <port id="60000" protocol="https">
      <interopnamespacelist>
        <interopnamespace name="interop"/>
      </interopnamespacelist>
    </port>
  </wbemportlist>
```

3. Salve o arquivo `wbemportlist.xml`.
4. Reinicie o serviço HP SIM: clique com o botão direito no serviço HP Systems Insight Manager e selecione **Reiniciar** na lista suspensa.

### Corrigir uma instalação existente do HP SIM

**Importante:** Não use o procedimento a seguir no caso de uma instalação inicial do HP SIM. Use esse procedimento somente se o HP SIM já tiver sido instalado e se a porta do WMI Mapper tiver sido alterada para algo (por exemplo, 6989) diferente do padrão (5989).

As seguintes etapas corretivas somente deverão ser executadas se o HP SIM já estiver instalado e se a porta do WMI Mapper tiver sido alterada para algo diferente do padrão de 5989.

Para restaurar a porta padrão do WMI Mapper:

1. Pare o serviço do Pegasus WMI Mapper.
2. Em um editor de texto, abra o arquivo: `C:\Program Files\The Open Group\WMI Mapper\cimserver_planned.conf`.
3. Na linha que inclui `httpsPort=6989`, altere o número da porta para **5989**.

   **Observação:** O número da porta pode ter sido definido como algo diferente de 6989. Ele é usado aqui somente como um exemplo.

4. Salve o arquivo.
5. Reinicie o serviço do Pegasus WMI Mapper.
6. Execute o comando `netstat` e verifique se que a alteração foi feita.

   ```
   C:\ netstat -anb >netstat.txt
   ```

   **Observação:** As alterações feitas no arquivo `cimserver_planned.conf` serão aplicadas ao arquivo `cimserver_current.conf` após a reinicialização do serviço.

Veja a seguir um exemplo do texto no arquivo `cimserver_planned.conf`.

```
enableRemotePrivilegedUserAccess=true
enableHttpsConnection=true
enableHttpConnection=false
sslCertificateFilePath=C:\hp\sslshare\cert.pem
sslKeyFilePath=C:\hp\sslshare\file.pem
httpsPort=5989
```

Para alterar a porta do Proxy do WMI Mapper no HP SIM:

1. Faça logon no HP SIM com privilégios administrativos.
2. Verifique se que as credenciais existentes do dispositivo host estão corretas:
   a. Abra a lista **Todos os sistemas** e selecione na lista o dispositivo que atua como CMS do HP SIM.
   b. Clique na guia **Ferramentas e links**.
   c. Clique no link **Credenciais do sistema**.
   d. Marque a caixa de seleção referente à instância CMS do WMI Mapper que está sendo executada no host local.
   e. Clique em **Editar credenciais do sistema**.
   f. Verifique se as credenciais de entrada existem e estão corretas para o CMS (preferencial) ou se existem configurações avançadas do WBEM. Além disso, verifique se o número da porta é 5989 e se as credenciais estão corretas para o WMI Mapper.
3. Na barra de navegação superior, selecione **Opções** → **Configurações de protocolo** → **Proxy do WMI Mapper**.
4. Selecione a instância CMS do WMI Mapper que está sendo executada no host local.
5. Clique em **Editar**.
6. Insira **5989** no campo **Número da porta**.
7. Clique em **OK** para salvar as configurações.

### *Restaurar padrões para o arquivo wbemportlist.xml*

1. Em um editor de texto, abra o arquivo: `C:\Program Files\HP\Systems Insight Manager\config\identification\wbemportlist.xml`
2. Remova as seguintes linhas do arquivo:

```
<!-- WMI Mapper httpsPort=6989 -->
<port id="6989" protocol="https">
  <cimnamespacelist>
    <cimnamespace name="root/cimv2"/>
  </cimnamespacelist>
</port>
```

3. Adicione as seguintes linhas ao final do arquivo. Neste exemplo, o número da porta 60000 é usado como a porta HTTPS para o SMI-S.

```
</port>
<port id="60000" protocol="https">
  <interopnamespacelist>
    <interopnamespace name="interop"/>
  </interopnamespacelist>
</port>
```

O exemplo a seguir mostra o arquivo completo, com o número de porta 60000 usado como a porta HTTPS para o SMI-S:

```
<?xml version="1.0" encoding="UTF-8"?>
<wbemportlist>
  <port id="5989" protocol="https">
    <cimnamespacelist>
      <cimnamespace name="root/cimv2"/>
      <cimnamespace name="vmware/esxv2"/>
      <cimnamespace name="root/hpq"/>
    </cimnamespacelist>
    <interopnamespacelist>
      <interopnamespace name="root/pg_interop"/>
      <interopnamespace name="root"/>
      <interopnamespace name="root/emulex"/>
      <interopnamespace name="root/qlogic"/>
      <interopnamespace name="root/ibm"/>
      <interopnamespace name="root/emc"/>
      <interopnamespace name="root/smis/current"/>
      <interopnamespace name="root/hitachi/dm51"/>
      <interopnamespace name="interop"/>
      <interopnamespace name="root/interop"/>
      <interopnamespace name="root/switch"/>
      <interopnamespace name="root/cimv2"/>
    </interopnamespacelist>
  </port>
  <port id="60000" protocol="https">
    <interopnamespacelist>
      <interopnamespace name="interop"/>
    </interopnamespacelist>
  </port>
</wbemportlist>
```

4. Salve o arquivo.
5. Reinicie o serviço HP SIM.
6. Selecione **Opções → Identificar sistemas** para identificar novamente todos os sistemas WBEM/WMI no HP SIM de forma a corrigir a referência de porta.

### Instalar e configurar o P6000 Command View após o HP SIM

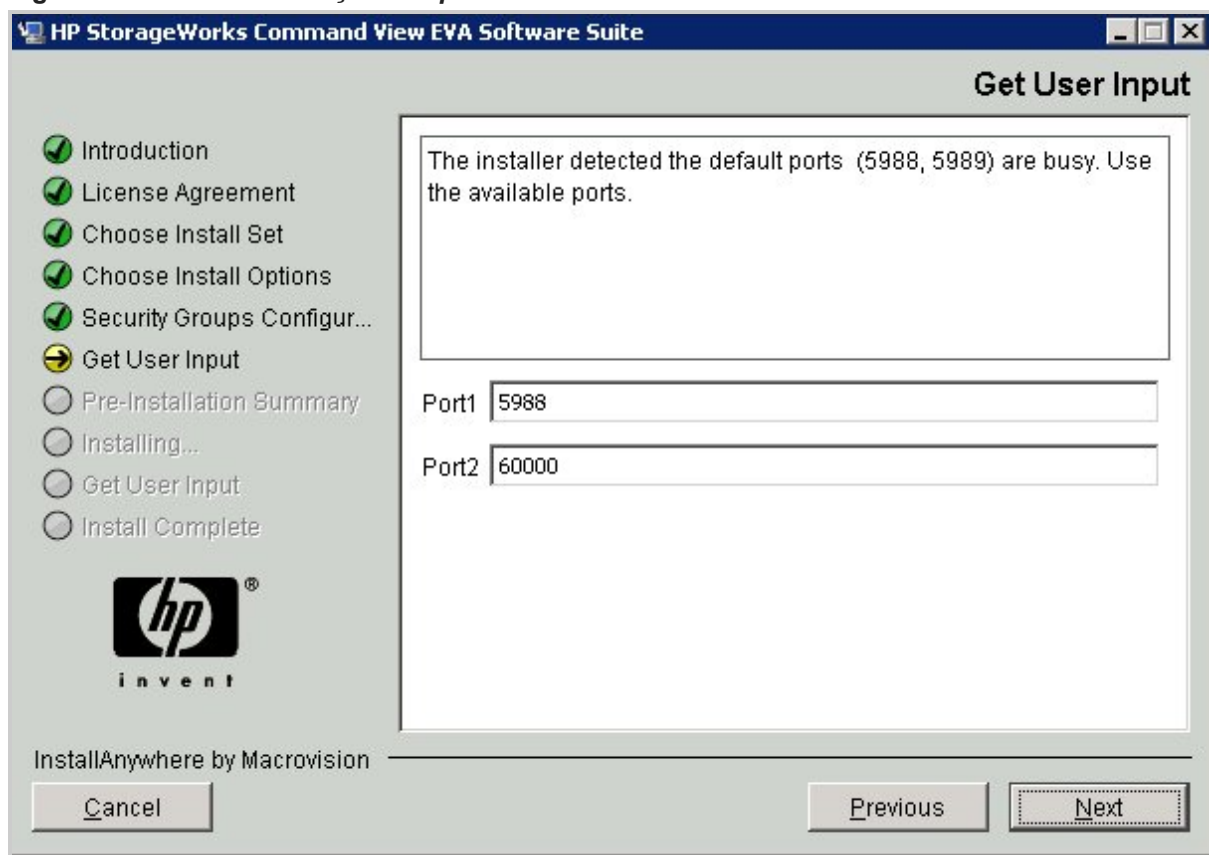
O kit de instalação do P6000 Command View inclui o SMI-S como componente. No momento da instalação, o SMI-S atribuirá as seguintes portas por padrão, se elas estiverem disponíveis:

- Porta HTTP =5988
- Porta HTTPS =5989

Se uma ou ambas as portas estiverem em uso, a instalação fornecerá uma tela de configuração adicional na qual você pode alterar os números das portas. O instalador do SMI-S sugerirá a porta 60000 se ela não estiver em uso. O SMI-S manterá a porta 5988 se ela não estiver em conflito com outro número de porta. O SMI-S usa essas portas quando o processo HP CIM Object Manager (CIMOM) é iniciado.

**Observação:** Essa tela somente será exibida se um conflito de porta for detectado. É por isso que a HP recomenda a instalação do HP SIM antes da instalação do Command View.

A figura a seguir mostra um exemplo de instalação do SMI-S em um dispositivo host do Insight RS que já possui o HP SIM instalado com o WMI Mapper:

**Figura 20.1** ***Tela de instalação complementar do SMI-S***

Uma vez configuradas as portas, você pode verificá-las executando o comando `netstat`:

```
C:\ netstat -anb >netstat.txt
```

A seguinte saída é exibida:

```
TCP 0.0.0.0,0:5988 0,0.0.0.0:0 LISTENING 1712 [JavaWrapper.exe]
TCP 0.0.0.0,0:5989 0,0.0.0.0:0 LISTENING 460 [WMIServer.exe]
TCP 0.0.0.0,0:60000 0,0.0.0.0:0 LISTENING 1712 [JavaWrapper.exe]
```

Neste exemplo, o SMI-S está configurado para usar as portas 5988 e 60000.

Para redefinir os números de porta se o P6000 Command View já estiver instalado:

1. Abra o seguinte arquivo:

   `C:\Program Files\Hewlett-Packard\SMI-S\CXWSCimom\config\cxws.properties`

2. Localize as entradas `cxws.http.port` e `cxws.https.port` e redefina-as para os seguintes valores:

   `cxws.http.port=5988`

   `cxws.https.port=60000`

3. Reinicie o serviço HP CIMOM.

### Documentação do P6000 Command View

A documentação do P6000 Command View está disponível em: http://h18006.www1.hp.com/products/storage/software/cmdvieweva/index.html. Nos links relacionados, clique no link **Suporte técnico/Manuais** e depois no link **Manuais** para visualizar a lista de manuais do P6000 Command View.

Os seguintes documentos são necessários para a instalação e configuração do P6000 Command View:

- *Guia de Instalação do HP P6000 Command View Suite*
- *Notas de versão do HP P6000 Command View Suite*
- *Referência de compatibilidade do HP P6000 Enterprise Virtual Array*

Para mais informações, visite *Visão geral das especificações da suíte de software HP StorageWorks HP P6000 Command View*, em: http://h18004.www1.hp.com/products/quickspecs/12239_div/12239_div.html

## Instalar o pacote de software do ELMC no servidor do P6000 Command View

O ELMC deve estar instalado no servidor do P6000 Command View, para permitir o acesso a dados de evento registrados em log da matriz. Antes, isso era chamado de servidor de gerenciamento de armazenamento (SMS).

O ELMC é necessário no servidor do P6000 Command View para que os eventos possam ser encaminhados ao Insight RS.

Se o ELMC já estiver instalado no servidor do P6000 Command View, certifique-se de que sua versão seja a 6.2 ou mais recente. Se a versão for anterior à 6.2, será preciso atualizá-la. Para verificar a versão do ELMC, execute o seguinte comando:`wccproxy version`.

**Observação:** Ao atualizar para o ELMC versão 6.4, o número de versão incorreto é mostrado na janela de atualização. Após a execução da atualização, o número de versão correto 6.4 aparecerá na janela Programas e recursos e quando você executar o comando `wccproxy version`.

Para instalar o pacote de software do ELMC, conclua as seguintes etapas:

1. No Insight RS Console, navegue até a guia **Configurações do administrador** → **Atualizações de software** e selecione o pacote de software *Coletor de Monitoramento do Log de Eventos (ELMC)*.
2. Na guia **Versão disponível**, clique em **Download**.
3. Quando o download for concluído, clique em **Instalar**. Os pacotes do ELMC são guardados na pasta `%HP_RS_DATA%\ELMC`. Por padrão, a pasta é `C:\ProgramData\HP\RS\DATA\ELMC`.

   **Observação**: A pasta `ProgramData` é uma pasta oculta. Para exibir essa pasta, defina as opções de pasta para mostrar pastas ocultas.
4. Copie o pacote de software apropriado do ELMC para Windows x86/x64 para um diretório temporário no servidor do P6000 Command View.
5. Dê um clique duplo no arquivo do instalador para iniciar o processo de instalação. O kit será instalado e encerrado sem prompts ao usuário. Não é necessário entrar com nenhuma configuração de usuário para instalar o pacote de software do ELMC.

## Definir configurações de firewall e porta

Para obter uma lista completa de requisitos de firewall e de porta para dispositivos monitorados, consulte o *Informe de Segurança do HP Insight Remote Support*, em: http://www.hp.com/go/insightremotesupport/docs.

# Adicionar credenciais de protocolo e iniciar a detecção

Para detectar seus dispositivos monitorados, conclua as seguintes seções:

## Criar um protocolo do P6000 Command View no Insight RS Console

Para configurar uma credencial protocolo P6000 no Insight RS Console, conclua as seguintes etapas:

1. Em um navegador da Web, faça logon no Insight RS Console.
2. No menu principal, selecione **Detecção** e clique na guia **Credenciais**
3. Na lista suspensa **Selecionar e configurar protocolo**, selecione **HP P6000 Command View**.
4. Clique em **Novo**. A caixa de diálogo Nova credencial é exibida.
5. Digite o nome de usuário e a senha para a instância do P6000 Command View.
6. Clique em **Adicionar**.

A HP recomenda também a criação de credenciais para o servidor no qual o software P6000 Command View está sendo executado.

## Criar um protocolo ELMC no Insight RS Console

Para configurar o ELMC no Insight RS Console, conclua as seguintes etapas:

1. Em um navegador da Web, faça logon no Insight RS Console.
2. No menu principal, selecione **Detecção** e clique na guia **Credenciais**.
3. Na lista suspensa **Selecionar e configurar protocolo**, selecione **Coletor de monitoramento do log de eventos (ELMC)**.
4. Clique em **Novo**. A caixa de diálogo Nova credencial é exibida.

O Insight RS cria a credencial de protocolo, que é exibida na tabela de credenciais.

## Detectar o comutador EVA no Insight RS Console

Um EVA não é detectado diretamente. O EVA é localizado ao se detectar o servidor P6000 Command View que está gerenciando o EVA.

**Importante:** Quando uma nova matriz EVA é adicionada a um ambiente do Insight RS que já esteja configurado, uma detecção manual do servidor que executa o P600 Command View que gerencia a nova matriz é necessária para a detecção das novas informações de garantia e contrato do EVA.

Para detectar o dispositivo por meio do Insight RS Console, conclua as seguintes etapas:

1. Em um navegador da Web, faça logon no Insight RS Console.
2. No menu principal, selecione **Detecção** e clique na guia **Fontes**.
3. Expanda a seção Endereços IP e adicione o endereço IP do seu dispositivo:
   a. Clique em **Novo**.
   b. Selecione **Endereço único**, **Intervalo de endereços** ou **Lista de endereços**.
   c. Digite os endereços IP dos dispositivos a serem detectados.
   d. Clique em **Adicionar**.
4. Clique em **Iniciar detecção**.

## Verificar o status de detecção e do dispositivo

Para verificar se o dispositivo foi detectado corretamente, conclua as seguintes etapas:

1. Em um navegador da Web, faça logon no Insight RS Console.
2. No menu principal, selecione **Dispositivos** e clique na guia **Resumo do dispositivo**.
3. Verifique se a coluna Status contém um ícone de êxito ( ).

   Se não houver ícone de êxito, tente descobrir que coluna está com problema e consulte a Ajuda on-line para informações de solução de problemas.

## Verificar informações de garantia e contrato

Verifique se as informações de garantia e contrato foram detectadas corretamente no Insight RS Console:

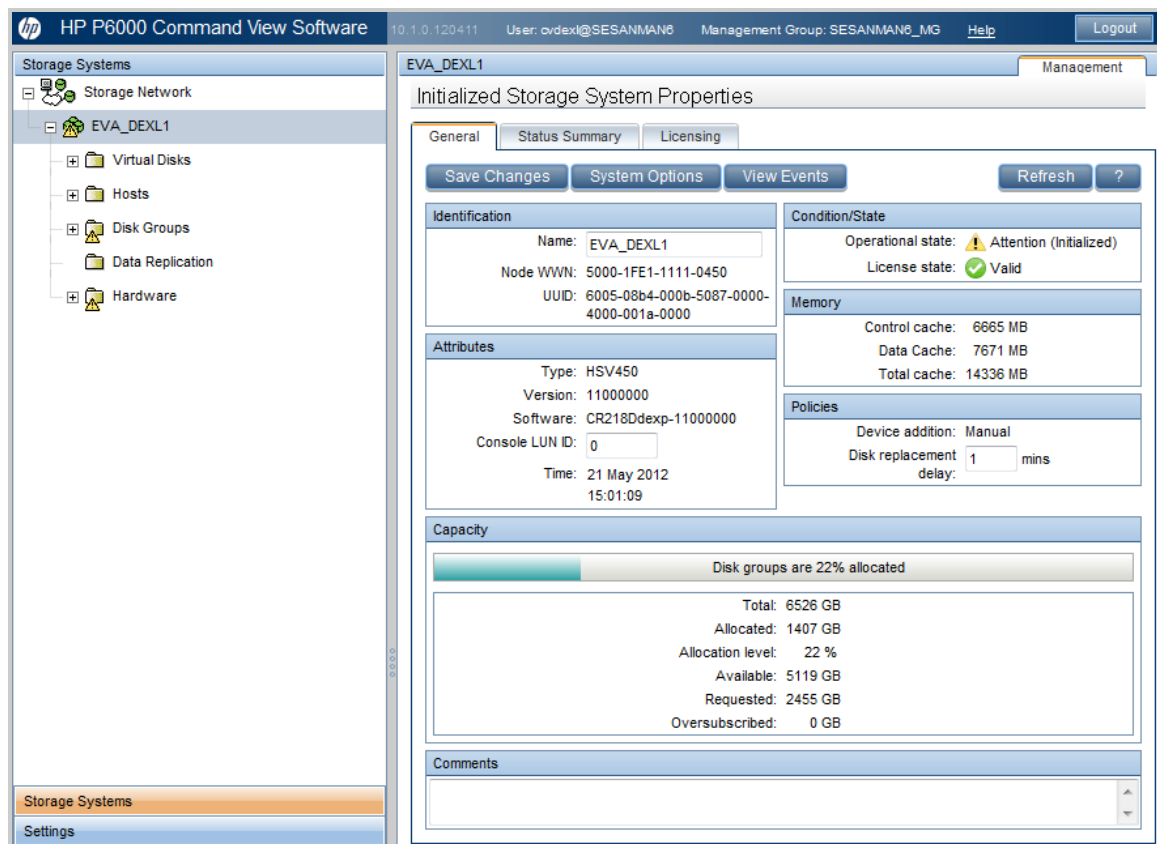
1. No Insight RS Console, navegue até **Dispositivos** e clique no Nome do dispositivo EVA.
2. Expanda a seção Hardware e confira se o **Número de série adquirido** e o **Número do produto adquirido** estão corretos. Se eles não estiverem corretos, digite os valores corretos nos campos **Substituir número de série** e **Substituir número do produto** e clique em **Salvar alterações**.

# Verificar a comunicação entre o dispositivo monitorado e o Insight RS

Para verificar a comunicação entre o dispositivo monitorado e o Insight RS, conclua as seguintes seções:

## Enviar um evento de teste

Para enviar um evento de teste do P6000 Command View, siga estas instruções:

1. Em um navegador da web, acesse o P6000 Command View.
2. No menu esquerdo, selecione o EVA.

3. Na guia **Geral**, clique em **Opções do sistema**.
4. Na tela Opções do sistema, sob o título **Serviço**, clique em **Realizar teste de serviço remoto**.

5. Na tela Realizar teste de serviço remoto, clique em **Realizar teste de serviço remoto**.
6. Clique em **OK**.
7. No Insight RS Console, navegue até **Dispositivos** → **Eventos de serviços** para verificar se o evento foi recebido.

### Verificar coletas no Insight RS Console

Coletas não são executadas automaticamente depois da descoberta. A HP recomenda que você execute uma coleta manualmente após a descoberta completa para verificar a conectividade. Execute o cronograma de coleta manualmente na guia Serviços de coleta → Agendamentos de coleta. Para obter mais informações sobre o agendamento de coletas, consulte a Ajuda do Insight RS.

Verifique se essa coleta foi bem-sucedida na guia Serviços de coleta → Resultados da Coleta de Armazenamento SAN no Insight RS Console.

1. Faça logon no Insight RS Console.
2. No menu principal, selecione **Serviços de coleta** e depois clique na guia **Resultados da Coleta de Armazenamento SAN**.
3. Expanda a seção Coleta de configurações de armazenamento.
4. Localize a entrada referente ao seu dispositivo e verifique a coluna Resultado. Se a coleta tiver sido bem-sucedida, um ícone de êxito será exibido ( ). Se ocorrer uma falha, um ícone de erro será exibido ( ).

## Manutenção e solução de problemas

### Habilitar o Modo de serviço iniciado pelo usuário no P6000 Command View

O Modo de serviço iniciado pelo usuário (UISM) fornece um meio de permitir que incidentes de serviços de diagnóstico do Remote Support sejam suprimidos ou revelados apenas para o cliente, permitindo que a tecnologia de diagnóstico do Remote Support continue a monitorar o dispositivo, gravando um 'Evento de serviço iniciado pelo usuário' no log do Dispositivo. O uso do UISM reduzirá o número de eventos não acionáveis que são criados quando durante a instalação ou manutenção do software.

O UISM é habilitado por meio do P6000 Command View. O UISM volta automaticamente ao modo normal depois que um tempo de retardo ajustável expira ou por desabilitação manual. Dois novos eventos de gerenciamento do P6000 Command View serão criados quando o UISM for habilitado. O primeiro indicará o início do UISM e conterá um valor de tempo limite em minutos dentro da descrição do evento. O segundo indicará o fim do UISM.

Estar nesse modo não tem nenhum efeito sobre a funcionalidade do P6000 Command View ou no tratamento de evento dentro do P6000 Command View. Esse modo é apenas para o benefício de ferramentas de apoio externas, como o Insight Remote Support.

Para habilitar o Modo de serviço iniciado pelo usuário, siga estas instruções:

1. Abra o P6000 Command View e selecione um dispositivo na árvore de menu à esquerda.
2. Na página Opções do sistema, sob o título**Serviço**, selecione **Configurar Modo de serviço**

**iniciado pelo usuário (UISM)**.

3. Na página Configurar Modo de serviço iniciado pelo usuário, digite um motivo para o UISM na área de texto **Motivo**.
4. Modifique a duração, se necessário. O padrão é 30 minutos.
5. Clique em **Iniciar modo de serviço**.
6. Na janela suspensa, clique em **Iniciar modo de serviço** para confirmar que você deseja acessar o UISM. A página Configurar modo de serviço iniciado pelo usuário será atualizada para mostrar que o UISM está ativo, o **Modo** terá mudado, e o tempo restante no UISM será exibido.
7. Se você quiser sair do UISM antes de a duração expirar, poderá clicar em **Interromper modo de serviço**.

## Executar um teste de serviço remoto no P6000 Command View

O teste de serviço remoto fornece um método para confirmar uma configuração de suporte remoto bem-sucedida e para solucionar problemas de comunicação de software. Quando um teste de serviço remoto é realizado, o Insight Remote Support recebe o evento e o envia à HP. A HP enviará o evento de volta para o usuário. Isso permite um teste de ponta a ponta, que pode ser usado para testar ou solucionar problemas no caminho de comunicação do software de suporte remoto. O teste do serviço remoto não tem outro efeito dentro do P6000 Command View além de registrar o evento e enviar as notificações configuradas.

Para executar um teste de serviço remoto, siga estas instruções:

1. Abra o P6000 Command View e selecione um dispositivo na árvore de menu à esquerda.
2. Na página Opções do sistema, sob o título **Serviço**, selecione **Realizar teste de serviço remoto**.
3. Na página Realizar teste de serviço remoto, clique em **Realizar teste de serviço remoto**.
4. Confirme se o evento de teste foi recebido no Insight RS Console.

# Configurar Enterprise Virtual Arrays e P6000 com o gerenciamento baseado em array

O EVA4400 e o P6000 podem ser monitorados com o uso do Gerenciamento baseado em array. A introdução do EVA4400 incluiu um novo módulo para o par controlador HSV300 que instala o Command View EVA no array. Isso é chamado Gerenciamento baseado em array (ABM), que tem uma interface de rede para acesso pela rede local. O ABM não é capaz de hospedar o SMI-S no array e, portanto, o SMI-S deve ser hospedado em outro lugar na rede local, para servir como uma conexão de proxy ao array.

O kit de instalação do P6000 Command View permite que o SMI-S seja instalado independentemente em um servidor designado. Instale o SMI-S no dispositivo host ou em outro servidor com suporte na rede local.

**Importante:** O nome do domínio totalmente qualificado do ABM não deve ser igual ao nome do array EVA. O Insight RS não tem como diferenciar entre dois dispositivos que possuem o mesmo nome.

# Atender aos requisitos de configuração

Para configurar Enterprise Virtual Arrays e P6000 usando o ABM para que eles sejam monitorados pelo Insight RS, conclua as seguintes seções:

**Tabela 20.2** ***Etapas de configuração de Enterprise Virtual Arrays e P6000 usando o ABM***

| Tarefa | Concluída? |
|---|---|
| Certifique-se de que o Insight RS suporte sua matriz de discos P6000, verificando o *Notas de Lançamento do HP Insight Remote Support*. | |
| Adicione o P6000 Command View ao Insight RS Console. | |
| Detecte o P6000 no Insight RS Console. | |
| Adicione o Tipo e o Identificador de suporte do dispositivo ao Insight RS Console. | |

# Configurar dispositivos monitorados

Para configurar seus dispositivos monitorados, conclua a seguinte seção:

## Definir configurações de firewall e porta

Para obter uma lista completa de requisitos de firewall e de porta para dispositivos monitorados, consulte o *Informe de Segurança do HP Insight Remote Support*, em: http://www.hp.com/go/insightremotesupport/docs.

## Adicionar credenciais de protocolo e iniciar a detecção

Para detectar seus dispositivos monitorados, conclua as seguintes seções:

### *Criar um protocolo do P6000 Command View no Insight RS Console*

Para configurar uma credencial protocolo P6000 no Insight RS Console, conclua as seguintes etapas:

1. Em um navegador da Web, faça logon no Insight RS Console.
2. No menu principal, selecione **Detecção** e clique na guia **Credenciais**
3. Na lista suspensa **Selecionar e configurar protocolo**, selecione **HP P6000 Command View**.
4. Clique em **Novo**. A caixa de diálogo Nova credencial é exibida.
5. Digite o nome de usuário e a senha para a instância do P6000 Command View.

   Configure as credenciais para o ABM que está executando o P6000 Command View e gerenciando ativamente a matriz. Se a matriz não estiver sendo gerenciada pela instância do P6000 Command View para a qual você está apontando, a matriz EVA estará visível, mas o Insight RS não conseguirá obter as informações de número de série ou de número de produto.
6. Clique em **Adicionar**.

### Detectar o comutador ABM no Insight RS Console

Se você estiver gerenciando a matriz na instância do P6000 Command View que está executando o gerenciamento baseado em matriz (ABM), você precisará detectar o ABM.

Para detectar o dispositivo por meio do Insight RS Console, conclua as seguintes etapas:

1. Em um navegador da Web, faça logon no Insight RS Console.
2. No menu principal, selecione **Detecção** e clique na guia **Fontes**.
3. Expanda a seção Endereços IP e adicione o endereço IP do seu dispositivo:
   a. Clique em **Novo**.
   b. Selecione **Endereço único**, **Intervalo de endereços** ou **Lista de endereços**.
   c. Digite os endereços IP dos dispositivos a serem detectados.
   d. Clique em **Adicionar**.
4. Clique em **Iniciar detecção**.
5. Após a detecção ser concluída com êxito, navegue até **Dispositivos**, no menu principal, e, na guia **Resumo do dispositivo**, clique no nome do dispositivo da matriz, para abrir a tela Detalhes do dispositivo.
6. Na guia **Dispositivo**, expanda a seção Garantia e contrato e digite o Tipo de suporte e o Identificador de suporte do dispositivo.
7. Clique em **Salvar alterações**, para salvar as informações.
8. Volte à tela **Dispositivos** e verifique o Status do dispositivo.

### Verificar o status de detecção e do dispositivo

Para verificar se o dispositivo foi detectado corretamente, conclua as seguintes etapas:

1. Em um navegador da Web, faça logon no Insight RS Console.
2. No menu principal, selecione **Dispositivos** e clique na guia **Resumo do dispositivo**.
3. Verifique se a coluna Status contém um ícone de êxito ( ).

   Se não houver ícone de êxito, tente descobrir que coluna está com problema e consulte a Ajuda on-line para informações de solução de problemas.

## Verificar a comunicação entre o dispositivo monitorado e o Insight RS

Para verificar a comunicação entre o dispositivo monitorado e o Insight RS, conclua a seguinte seção:

### Verificar coletas no Insight RS Console

Coletas não são executadas automaticamente depois da descoberta. A HP recomenda que você execute uma coleta manualmente após a descoberta completa para verificar a conectividade. Execute o cronograma de coleta manualmente na guia Serviços de coleta → Agendamentos de coleta. Para obter mais informações sobre o agendamento de coletas, consulte a Ajuda do Insight RS.

Verifique se essa coleta foi bem-sucedida na guia Serviços de coleta → Resultados da Coleta de Armazenamento SAN no Insight RS Console.

1. Faça logon no Insight RS Console.
2. No menu principal, selecione **Serviços de coleta** e depois clique na guia **Resultados da Coleta de Armazenamento SAN**.
3. Expanda a seção Coleta de configurações de armazenamento.
4. Localize a entrada referente ao seu dispositivo e verifique a coluna Resultado. Se a coleta tiver sido bem-sucedida, um ícone de êxito será exibido ( ). Se ocorrer uma falha, um ícone de erro será exibido ( ).

# Capítulo 21: Configurar sistemas de armazenamento StoreVirtual P4000

O software HP Insight Remote Support oferece suporte remoto seguro para seus servidores HP, armazenamento, rede e ambientes SAN, que agora incluem o P4000 SAN.

**Observação:** HP StoreVirtual Storage é o novo nome das soluções de armazenamento HP LeftHand e HP P4000 SAN. Sistema operacional LeftHand (LeftHand OS) é o novo nome para SAN/iQ.

**Importante:** Cada nó de armazenamento P4000 é contado como 30 dispositivos monitorados no Insight RS.

**Importante:** Para cada 100 dispositivos P4000 que estão monitorados pelo Insight RS, acrescente 1 GB de espaço livre em disco para atender aos requisitos do dispositivo host.

Documentação adicional sobre o P4000 está disponível em: http://www.hp.com/support/manuals. Na seção **Armazenamento**, clique em **Sistemas de armazenamento em disco** e selecione **Soluções de SAN HP LeftHand P4000**.

## Atender aos requisitos de configuração

Para configurar seus sistemas de armazenamento P4000 de forma que eles sejam monitorados pelo Insight RS, conclua as seguintes seções:

**Tabela 21.1** ***Etapas da configuração do sistema P4000 Storage***

| Tarefa | Concluída? |
|---|---|
| Certifique-se de que o Insight RS suporte seu sistema de armazenamento P4000, verificando o *Notas de Lançamento do HP Insight Remote Support*. | |
| Instale ou atualize o CMC no dispositivo host. | |
| Instale ou atualize o LeftHand OS no P4000. | |
| Configure o SNMP no P4000. | |
| Adicione o protocolo da solução SAN (SAN/iQ) P4000 ao Insight RS Console. | |
| Detecte o sistema de armazenamento P4000 no Insight RS Console. | |
| Envie um evento de teste para verificar a conectividade entre seu sistema de armazenamento P4000 e o Insight RS. | |

## Instalar e configurar o software de comunicação em sistemas de armazenamento

Para configurar seus dispositivos monitorados, conclua as seguintes seções:

# Instalar e configurar o CMC no dispositivo host

Você precisará fazer a instalação completa do Console de gerenciamento centralizado (CMC) para instalar os SNMP MIBs. Se você não modificar os padrões SNMP usados pelo CMC, o SNMP funcionará com o Insight Remote Support sem modificações.

O Insight RS oferece suporte ao CMC 9.0 e versões superiores (o CMC 11.0 é recomendado).

O CMC 11.0 pode ser usado para gerenciar nós de armazenamento LeftHand OS 9.5, 10.x e 11.0.

O CMC, na versão para Windows, tem os seguintes requisitos:

**Tabela 21.2** ***Requisitos de memória e armazenamento para o CMC***

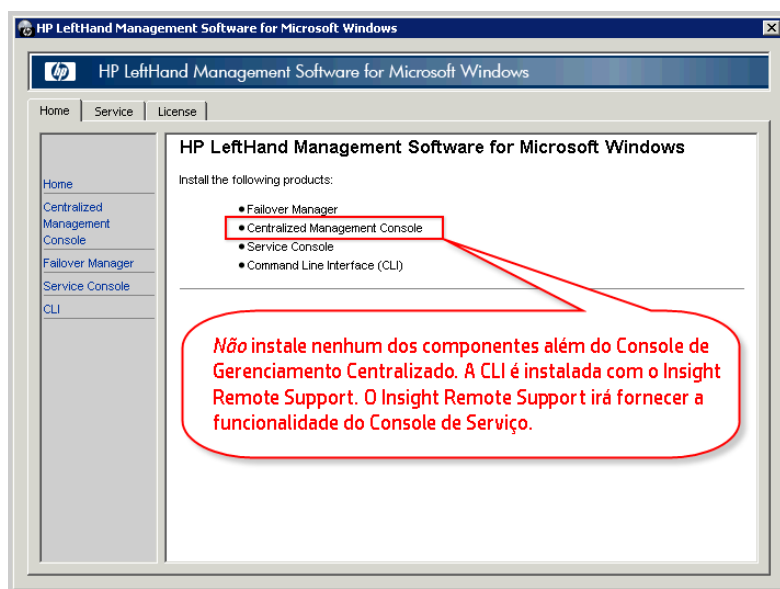
| Tamanho da memória | Espaço livre em disco |
|---|---|
| 100 MB de RAM durante o tempo de execução | 150 MB de espaço em disco para instalação completa |

**Observação:** O CMC pode ser instalado no dispositivo host ou ser instalado em um sistema à parte. Se o CMC já estiver instalado em outro sistema, não é necessário instalá-lo no dispositivo host.

Instale o console de gerenciamento centralizado (CMC) no computador que será usado para administrar o SAN. É necessário ter privilégios de administrador para instalar o CMC.

1. Insira o DVD do software de gerenciamento do P4000 na unidade de DVD. O instalador deve se iniciar automaticamente. Ou acesse o arquivo executável (`:\GUI\Windows\Disk1\InstData\VM\CMC_Installer.exe`)

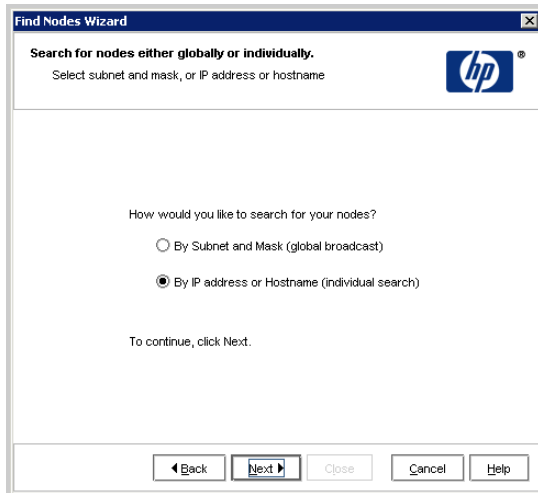
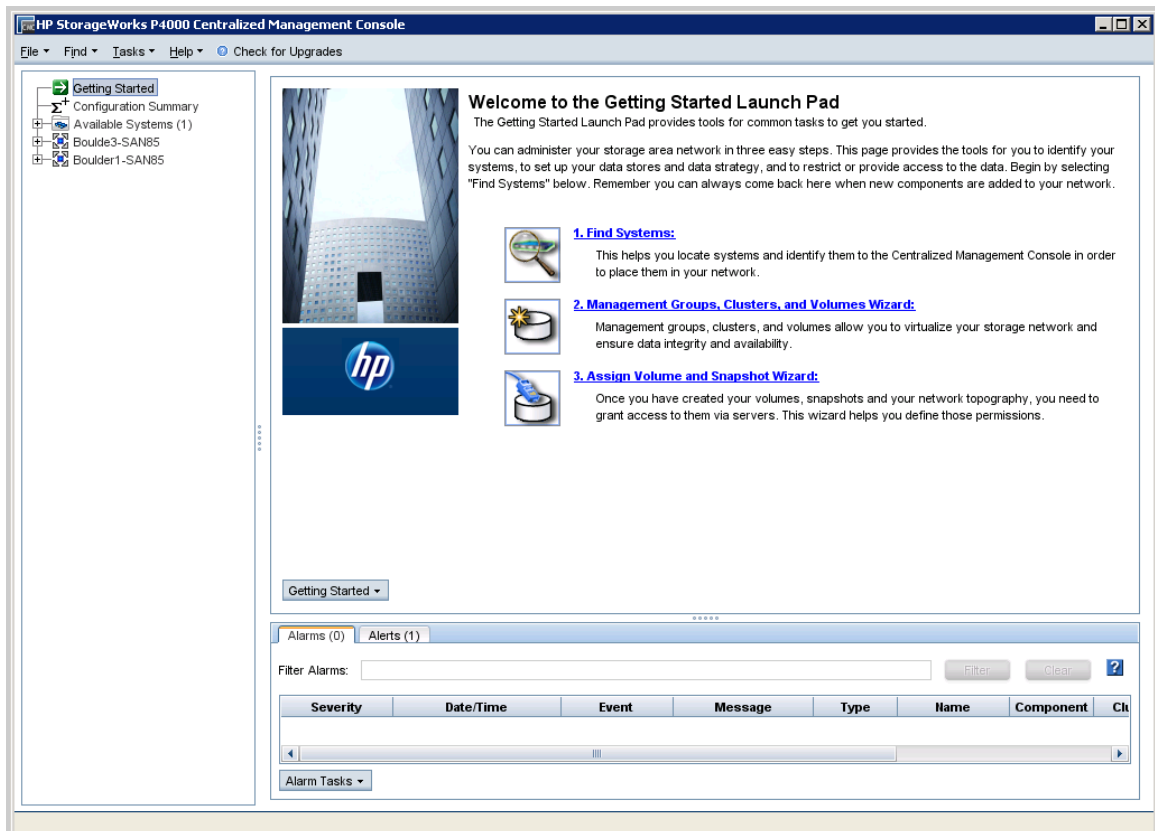
   Ou baixe o CMC em: http://www.hp.com/go/P4000downloads.

   Clique na opção de **Instalação completa**, que é recomendada para usuários que usam o SNMP.

   
   

   **Observação:** Se você já tiver o Console de Serviços instalado, não precisará desativá-lo.

O Insight Remote Support pode coexistir com o Console de Serviço sem conflitos.

2. Use o assistente Detectar nós para detectar os sistemas de armazenamento na rede, usando endereços IP ou nomes de host, ou usando a máscara de sub-rede e gateway da rede de armazenamento.

Os sistemas de armazenamento encontrados serão exibidos na categoria disponível no CMC.

# Atualizar o LeftHand OS nos sistemas de armazenamento P4000

**Observação:** Sistema operacional LeftHand (LeftHand OS) é o novo nome para SAN/iQ.

Use o CMC para atualizar para o LeftHand OS 9.5 ou superior (LeftHand OS 11.0 recomendado) nos sistemas de armazenamento P4000. Se os seus Sistemas de Armazenamento P4000 já têm o LeftHand OS 9.5 instalado, *não* será necessário realizar este procedimento.

**Observação:** Para dispositivos LeftHand OS 9.5, o Patch Set 05 é necessário para todos os dispositivos.

O CMC versão 9.0 e superiores trazem uma nova opção para fazer o download de atualizações e patches para o LeftHand OS a partir da HP. Após as atualizações e patches atuais serem baixados da HP para o sistema CMC, o CMC pode ser usado para atualizar os grupos de gerenciamento ou os nós com essas alterações.

Quando o software LeftHand OS é atualizado em um nó de armazenamento, o número de versão muda. Verifique a versão atual do software selecionando um nó de armazenamento na janela de navegação e visualizando a janela da guia Detalhes.

**Observação:** Atualizar diretamente do LeftHand OS 9.5 para o LeftHand OS 11.0 não é suportado.

**Importante:** Ao se instalar/atualizar o LeftHand OS, não modifique as configurações SNMP padrão. As configurações padrão são usadas pelo Insight Remote Support, e a comunicação entre o Sistema de Armazenamento P4000 e o dispositivo host não funcionará corretamente se as configurações SNMP forem modificadas. O SNMP é ativado por padrão no LeftHand OS. Observe que, no CMC 9.0, as armadilhas SNMP são configuradas no nível do grupo de gerenciamento, não no nível do nó.

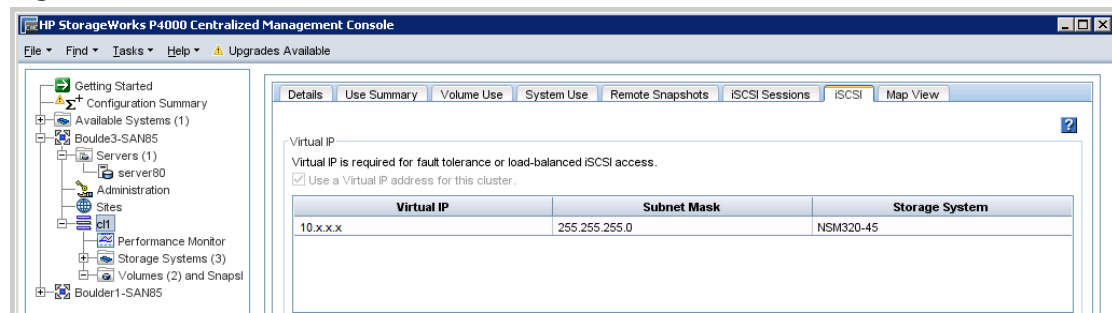
## *Noções básicas das melhores práticas*

- **Atualização do LSMD** — A atualização do LSMD é necessária para a atualização do SO LeftHand 7.x.
- **Endereços IP virtuais** — se um endereço IP Virtual (VIP) é atribuído a um nó de armazenamento em um cluster, o nó de armazenamento VIP precisa ser atualizado por último. O nó de armazenamento VIP aparece na guia de cluster iSCSI, mostrada na figura "Encontrar o nó de armazenamento executando o VIP".

  a. Atualize os nós de armazenamento não-VIP que estão executando gerenciadores, um por vez.

  b. Atualize os nós não-VIP e que não executam um gerenciador de armazenamento.

  c. Atualize o nó de armazenamento VIP.

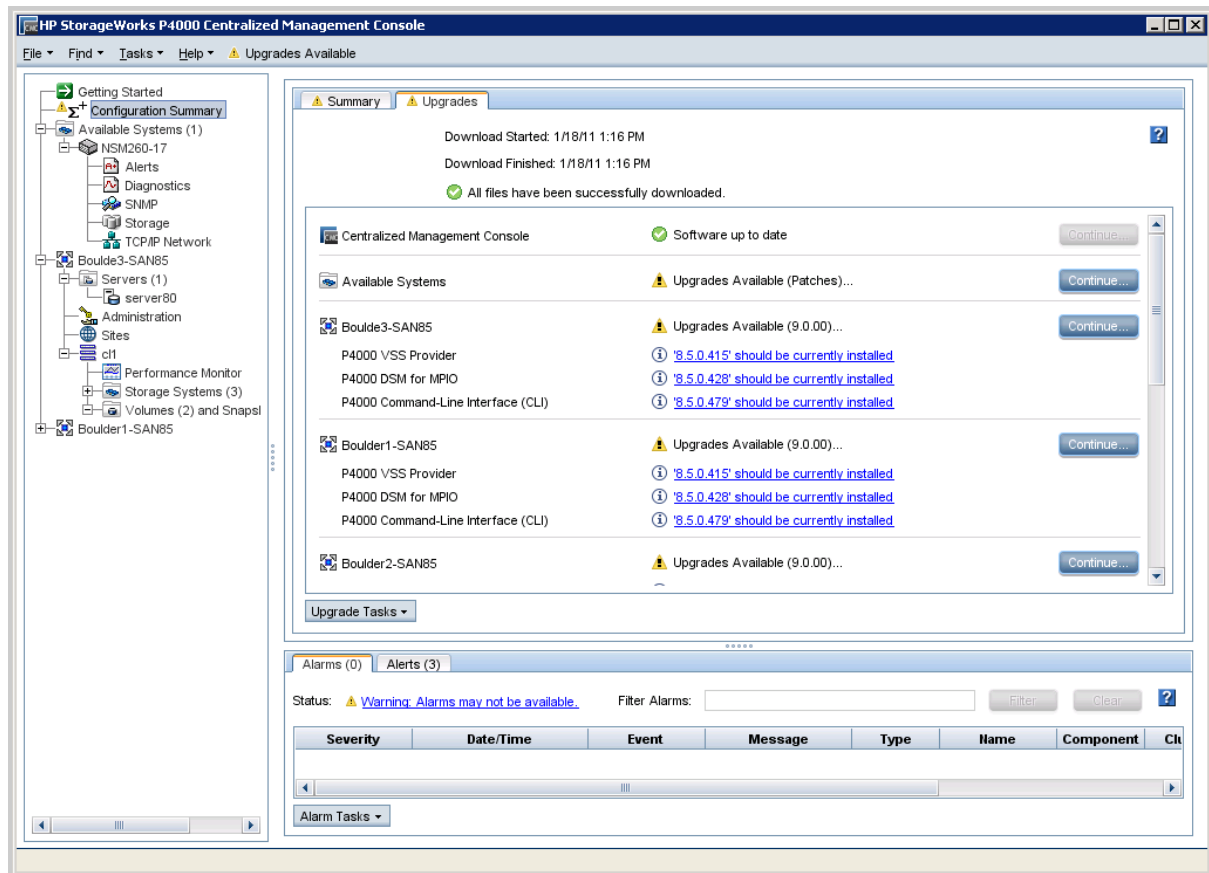
**Figura 21.1** ***Detectar o nó de armazenamento executando o VIP***

- **Cópia remota** — Se os grupos de gerenciamento estiverem sendo atualizados com associações a cópia remota, é necessário atualizar primeiro os grupos de gerenciamento remotos. Se o grupo principal for atualizado primeiro, a cópia remota pode parar de funcionar temporariamente até que o grupo de gerenciamento primário e o grupo remoto terminem a atualização. Atualize o site primário imediatamente após a atualização do site remoto. Consulte "Como verificar a versão do grupo de gerenciamento".

# *Selecionar o tipo de atualização*

O CMC suporta dois métodos de atualizações, conforme a figura “Exibir a janela de atualização/instalação do CMC”.

- Um por vez (recomendado) - Esse é o **método padrão e o único que deve ser usado se os nós de armazenamento estiverem em um grupo de gerenciamento**.
- Simultâneo (avançado) - Permite que múltiplos nós de armazenamento sejam atualizados ao mesmo tempo se eles não estiverem em um grupo de gerenciamento. Use apenas para nós de armazenamento no pool disponível.

**Cuidado:** Não selecione “Simultâneo (avançado)" se os nós de armazenamento estiverem em um cluster de produção.

**Figura 21.2** ***Exibir a janela de atualização/instalação do CMC***

# Aumentar o tamanho do disco do sistema operacional nos VSAs

Devido a alterações no tamanho das ferramentas VMware que são instaladas durante atualizações de software de versões anteriores à versão 8.5 do SO LeftHan, é necessário aumentar o tamanho do disco do SO antes de atualizar o VSA. As exigências de espaço adicional também são necessárias para versões futuras do software. Portanto, recomenda-se o aumento do tamanho do disco do SO para acomodar ambos os requisitos neste momento.

**Observação:** Estas instruções se aplicam ao VMware ESX Server. Outros produtos VMware têm instruções semelhantes para ampliar um disco virtual. Por favor, consulte a documentação do VMware apropriado para o produto que está sendo usado.

Para aumentar o tamanho do disco do sistema operacional no VSA, siga estas instruções:

1. Usando o CMC, desligue o VSA.
2. Abra o Cliente VI e selecione **VSA** → **Editar configurações** → **Hardware**.
3. Selecione o disco rígido 1 (verifique se o nó do dispositivo virtual é SCSI (0:0)).
4. Em Provisionamento de disco, altere o tamanho provisionado para 8 GB.

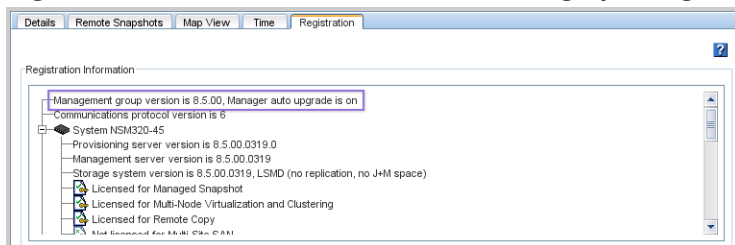
5. Clique em **OK**.
6. Repita essas etapas para o disco rígido 2 (verifique se o nó do dispositivo virtual é SCSI (0:1))
7. Usando o Cliente VI, ligue o VSA.
8. Detecte o VSA no CMC e aplique a atualização.

## *Verificar a versão do grupo de gerenciamento*

- Ao se atualizar o LeftHand da versão 7.x para a 9.5 ou 9.5, a versão do grupo de gerenciamento não passará à nova versão até que todos os nós de armazenamento no grupo de gerenciamento (e no grupo de gerenciamento remoto, se houver uma relação de cópia remota) forem atualizados para a versão do LeftHand OS 9.5 ou superior.
- Ao se atualizar da versão LeftHand OS 7.x para a 9.5 ou superior, o processo de atualização de hardware valida a identidade de todos os nós de armazenamento no grupo de gerenciamento. Se a validação falhar por qualquer motivo, a versão do grupo de gerenciamento não será atualizada para o 9.5 ou superior. Por exemplo, se um grupo de gerenciamento tiver uma combinação de plataformas, algumas das quais sem suporte por uma versão de software, então apenas as plataformas com suporte serão atualizadas com êxito. A versão do grupo de gerenciamento não será atualizada se as plataformas sem suporte permanecerem nesse grupo de gerenciamento.

Para verificar a versão do grupo de gerenciamento, conclua as seguintes etapas:

1. Na janela de navegação do CMC, selecione o grupo de gerenciamento e selecione a guia **Registro**. O número da versão do grupo de gerenciamento encontra-se na parte superior da seção Informações de registro, conforme a figura "Verificar o número de versão do grupo de gerenciamento".

**Figura 21.3** ***Verificar o número de versão do grupo de gerenciamento***

## *Verificar se há patches*

Depois de ter atualizado o LeftHand OS, use o CMC para verificar se há patches aplicáveis requeridos para o seu nó de armazenamento. O CMC 9.0 e superiores mostrarão os patches disponíveis e podem ser usados para baixá-los da HP para o sistema CMC.

# Configurar o SNMP no sistema de armazenamento P4000

Use o procedimento abaixo para verificar as configurações SNMP. Se você não modificou as configurações do SNMP do LeftHand OS ao instalar/atualizar o LeftHand OS, não deve ser necessário fazer qualquer atualização durante o procedimento a seguir.

Com o LeftHand OS, você pode configurar vários níveis de Alerta de severidade para enviar do grupo de gerenciamento. No Insight Remote Support, configure cada grupo de gerenciamento para enviar interceptações SNMP v1 dos níveis `Crítico` e `Aviso` em mensagens de texto com comprimento `Padrão`.

Os grupos de gerenciamento do LeftHand OS 9.5 e superiores configuram o destino do host de armadilha do dispositivo host SNMP quando estão no nível do grupo de gerenciamento. Mesmo que você configure apenas o SNMP no nível de grupo de gerenciamento, no CMC 10.0 ou superiores, é necessário configurar o SNMP no dispositivo host, para permitir armadilhas de todos os nós do LeftHand OS.

**Observação:** Para grupos de gerenciamento do LeftHand OS, os usuários podem configurar o comando **createSNMPTrapTarget** de destino do host de armadilha do dispositivo host P4000 CLI, em vez de usar CMC. O comando **getGroupInfo** exibirá as configurações atuais e destinos de interceptação do host do SNMP configurados no nível de grupo de gerenciamento.

**Observação:** se for usar os comandos P4000 CLI (CLIQ) **createSNMPTrapTarget** ou **getGroupInfo**, a variável do ambiente do caminho não será atualizada quando o P4000 CLI for instalado com o Insight RS. Será preciso usar o caminho completo com o P4000 CLI, que é `[Pasta_de_instalação_do_InsightRS]\P4000`.

Para verificar e/ou atualizar suas configurações SNMP, siga estas instruções:

1. Abra o CMC.
2. Verifique se o SNMP está habilitado para cada sistema de armazenamento:

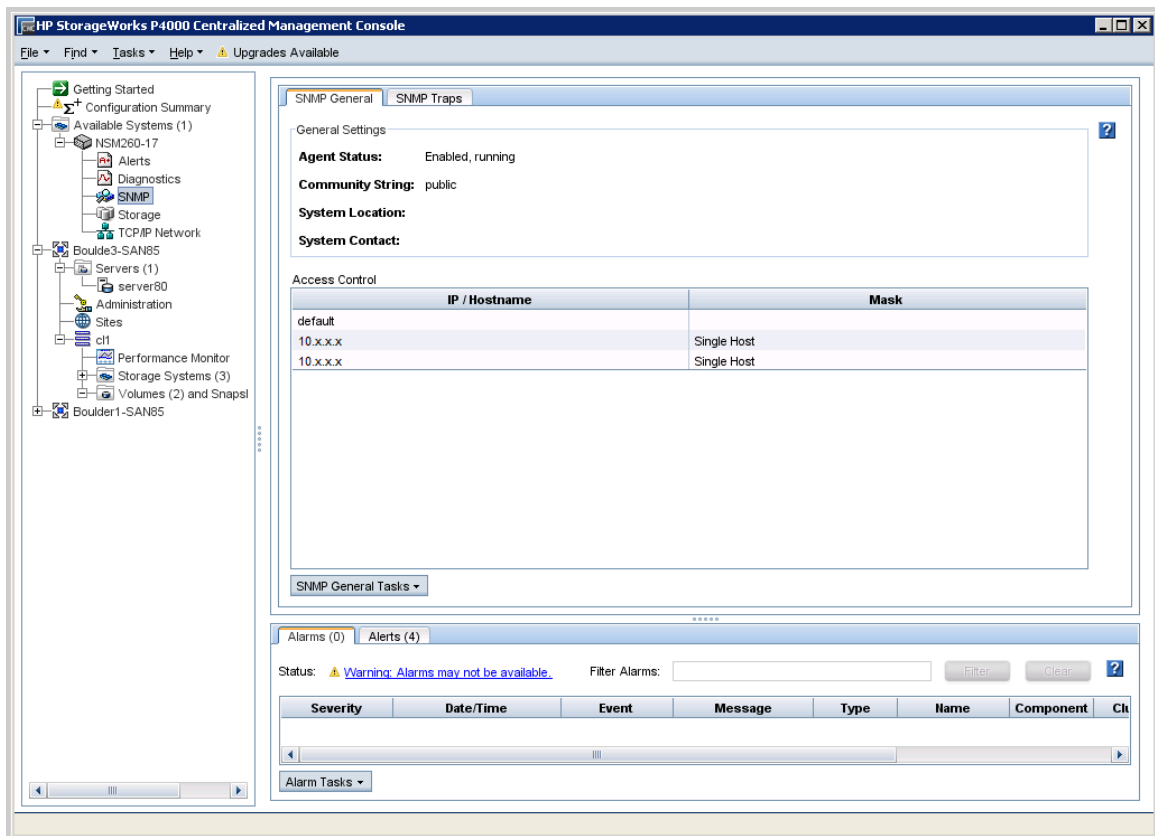
   

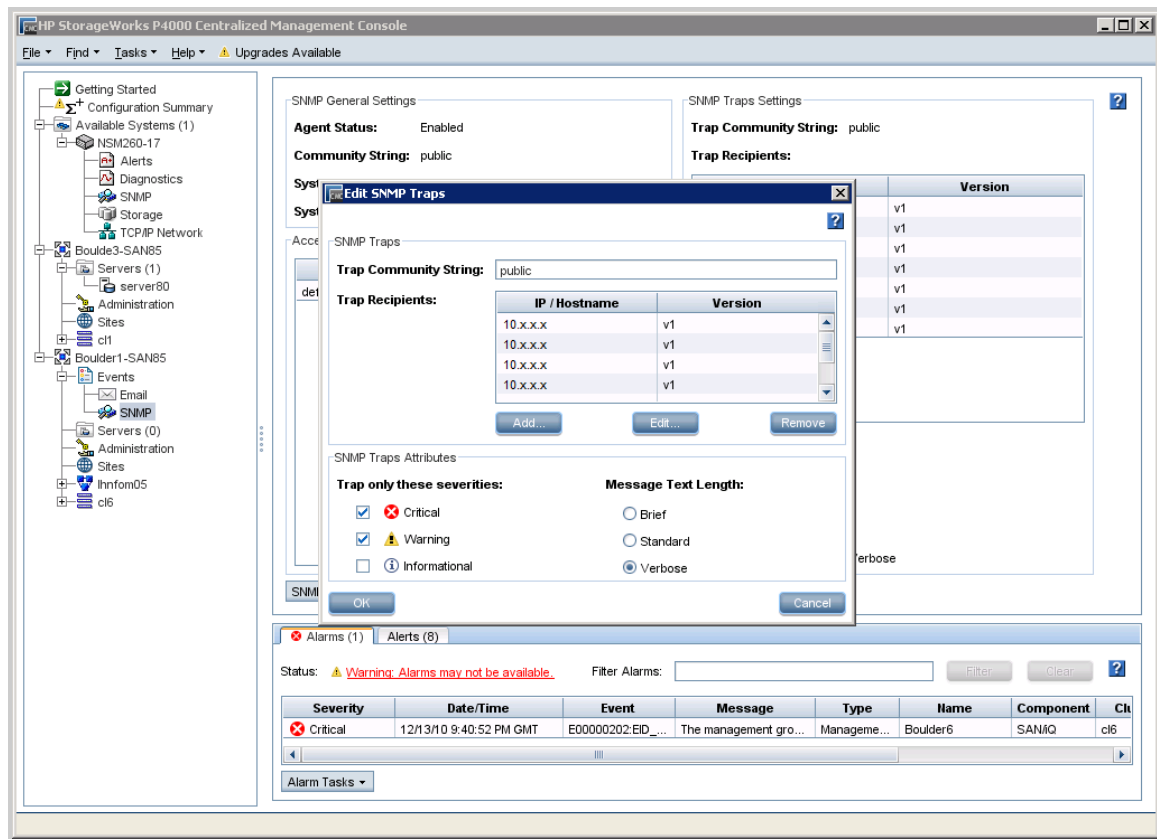
   **Observação:** O LeftHand OS, por padrão, vem de fábrica com o SNMP habilitado para todos os sistemas de armazenamento e configurado com a lista "padrão" de controle de acesso.

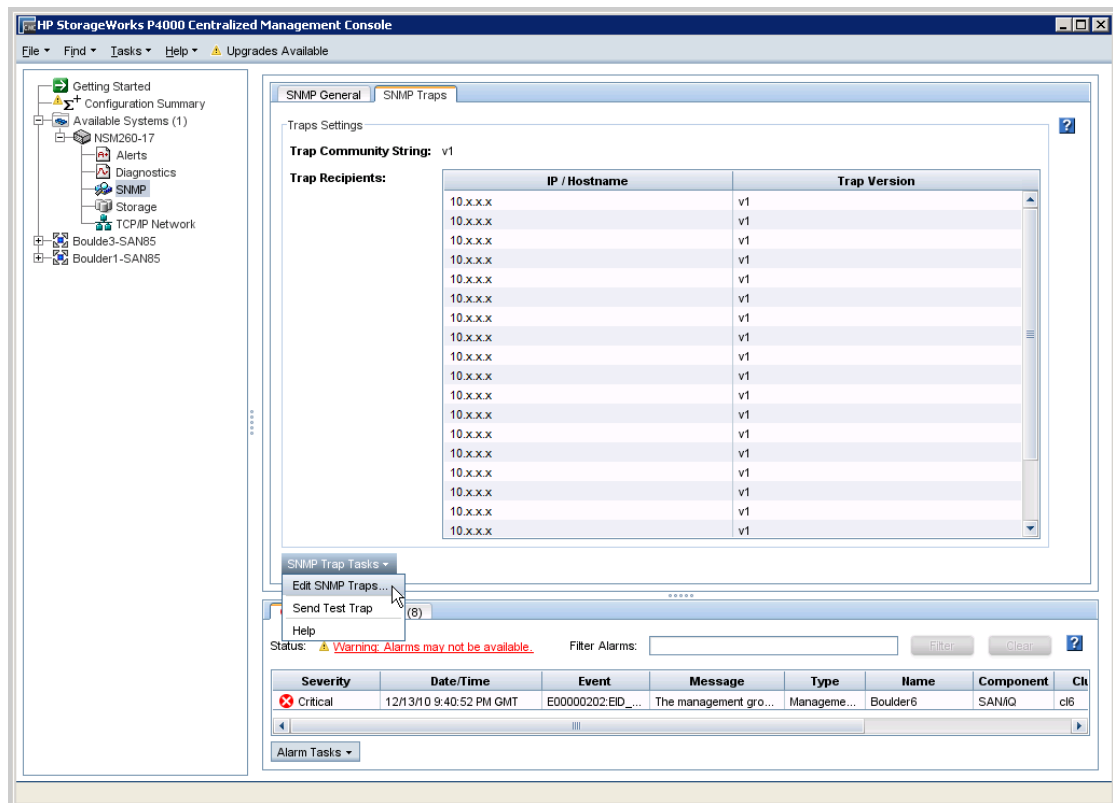
   **Observação:** Os grupos de gerenciamento do LeftHand OS configuram o destino do host de armadilha do dispositivo host SNMP quando estão no nível do grupo de gerenciamento. Com o LeftHand OS, você pode configurar vários níveis de Alerta de severidade para enviar do grupo de gerenciamento. No Insight Remote Support, configure cada grupo de gerenciamento para enviar interceptações SNMP v1 dos níveis `Crítico` e `Aviso` em mensagens de texto com comprimento `Padrão`.

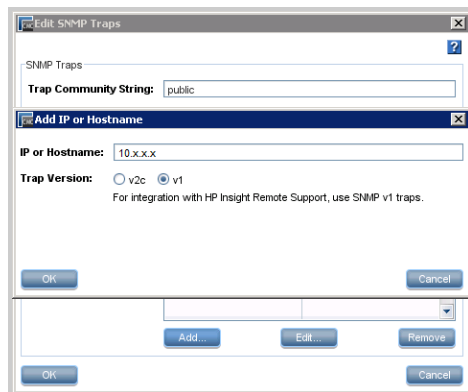
   a. Selecione **SNMP** na árvore de menu à esquerda e abra a guia **SNMP geral**.
   b. Verifique se o Status do agente é habilitado.
   c. Verifique se a cadeia de caracteres de comunidade SNMP do sistema de armazenamento P4000 está definida como `public` ou se com o mesmo valor configurado no Insight RS Console para detecção SNMP.
   d. No campo de controle de acesso, verifique se está listado `Padrão` ou o endereço IP do dispositivo host. A opção `Padrão` configura o SNMP para ser acessado pela cadeia de caracteres de comunidade `public` para todos os endereços IP.

**Observação:** As configurações SNMP nos sistemas de armazenamento P4000 precisam corresponder às configurações SNMP no dispositivo host.

3. **Selecione** Alertas na árvore de menu à esquerda e verifique se os alertas estão configurados com a opção “armadilha” para cada sistema de armazenamento.

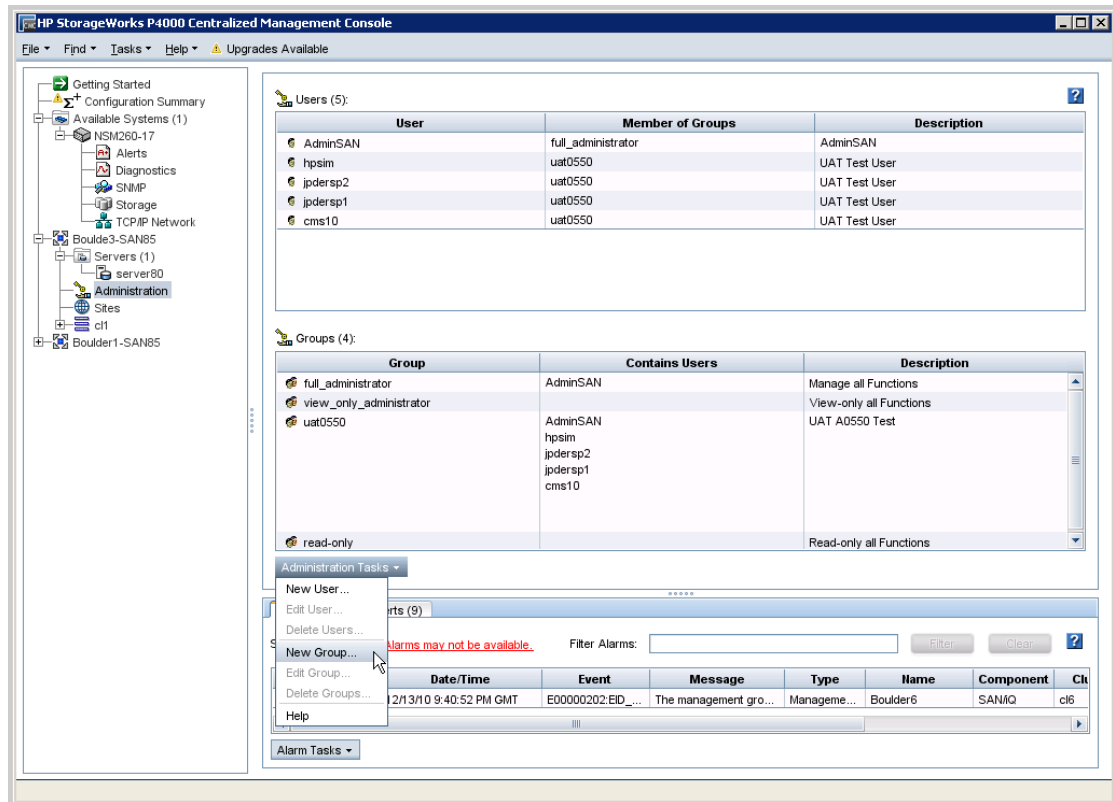
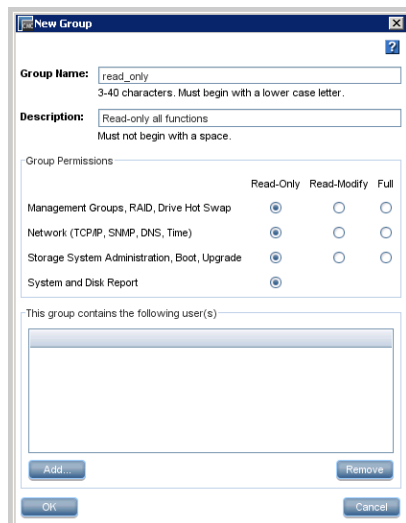
**Observação:** O LeftHand OS vem, por padrão, com armadilhas definidas para todos os casos de alerta.

4. Adicione o endereço IP do dispositivo host à lista de envios de armadilhas SNMP do sistema de armazenamento P4000. O endereço IP do dispositivo host é necessário para configurar armadilhas SNMP em cada sistema de armazenamento. Observe que no CMC 9.0 e superiores, as armadilhas SNMP são configuradas no nível do grupo de gerenciamento, não no nível do nó.

   a. Selecione **SNMP** na árvore de menu à esquerda e abra a guia **Armadilhas SNMP**.

   b. Abra a caixa de diálogo Editar armadilhas SNMP, acessando **Tarefas de armadilha SNMP** → **Editar armadilhas SNMP**.

c. Na caixa de diálogo Editar armadilhas SNMP, clique em **Adicionar**.

d. Na caixa de diálogo Adicionar IP ou Nome do host, digite o endereço IP ou o nome do host no campo **IP ou nome do host**. Verifique se a **Versão da interceptação** é v1 e clique em **OK**.

5. Repita os passos 3 e 4 para cada Sistema de Armazenamento P4000. Se preferir, também é possível configurar um nó usando as etapas 3 e 4 e então usar a opção de cópia de configuração do nó do CMC para copiar a configuração de todos os outros nós.

6. Incluir um usuário CMC adicional com credenciais somente de leitura. Isso é recomendado se você não desejar que o administrador do sistema do dispositivo host tenha controle para criar/excluir nos sistemas de armazenamento.

a. Selecione **Administração** na árvore de menu à esquerda.

b. Crie um grupo de usuários com acesso somente de leitura, se já não existir um. Navegue até **Tarefas administrativas** → **Novo grupo**.

c. Crie um novo usuário. Selecione o grupo criado na etapa anterior e prossiga para **Tarefas administrativas** → **Novo usuário**. Digite o nome de usuário, a senha e clique em **Adicionar** para adicionar esse usuário ao grupo de usuários com acesso somente de leitura criado.

# Definir configurações de firewall e porta

Para obter uma lista completa de requisitos de firewall e de porta para dispositivos monitorados, consulte o *Informe de Segurança do HP Insight Remote Support*, em: http://www.hp.com/go/insightremotesupport/docs.

# Adicionar credenciais de protocolo e iniciar a detecção

Para detectar seus dispositivos monitorados, conclua as seguintes seções:

## Adicionar o protocolo da solução SAN (SAN/iQ) P4000 ao Insight RS Console

Para adicionar o protocolo da solução SAN (SAN/iQ) P4000, siga estas instruções:

1. Em um navegador da web, faça logon no Insight RS Console (`https://`*<ip_ou_fqdn_do_dispositivo_host>*`:7906`.)
2. Crie uma credencial nomeado para cada conjunto de credenciais do grupo de gerenciamento:
   a. No Insight RS Console, navegue até **Informações da empresa** → **Credenciais nomeadas**.
   b. Clique em **Adicionar nova credencial**.
   c. Digite um nome para a credencial.
   d. Na lista suspensa **Protocolo**, selecione **P4000 SAN Solution (SAN/iQ)**.
   e. Digite o nome de usuário e a senha do grupo de gerenciamento criado em "Configurar o SNMP no sistema de armazenamento P4000". Essas credenciais podem ser completas para o grupo de

gerenciamento ou somente leitura do LeftHand OS.

   f. Clique em **Salvar info**.

3. Adicione as credenciais de detecção para os dispositivos P4000:
   a. No Insight RS Console, navegue até **Detecção** → **Credenciais**.
   b. Crie credenciais de protocolo de detecção para cada Credencial nomeada criada anteriormente.
      i. Na lista suspensa **Selecionar e configurar protocolo**, selecione **P4000 SAN Solution (SAN/iQ)**.
      ii. Clique em **Novo**.
      iii. Na lista suspensa **Credencial nomeada**, selecione a Credencial nomeada criada anteriormente.
      iv. Clique em **Adicionar**.

# Detectar o comutador P4000 no Insight RS Console

Para detectar o dispositivo por meio do Insight RS Console, conclua as seguintes etapas:

1. Em um navegador da Web, faça logon no Insight RS Console.
2. No menu principal, selecione **Detecção** e clique na guia **Fontes**.
3. Expanda a seção Endereços IP e adicione o endereço IP do seu dispositivo:
   a. Clique em **Novo**.
   b. Selecione **Endereço único**, **Intervalo de endereços** ou **Lista de endereços**.
   c. Digite os endereços IP dos dispositivos a serem detectados.

**Observação:** Ao detectar novos dispositivos P4000, não inclua endereços IP virtuais (VIP) do grupo de gerenciamento do P4000. Os endereços VIP são criados quando você cria e configura clusters do P4000. Em vez disso, detecte dispositivos P4000 usando endereços IP individuais ou crie intervalos de detecção excluindo todos os endereços VIP do P4000.

Se você detectar um endereço VIP do P4000, exclua a entidade gerenciada para o endereço VIP no Insight Remote Support Advanced, antes de executar quaisquer coletas ou capturar armadilhas de teste. Após excluir a entidade de endereço VIP, detecte novamente o nó, usando o endereço IP real do dispositivo P4000.

   d. Clique em **Adicionar**.

4. Clique em **Iniciar detecção**.

**Observação:** O Insight RS filtra dispositivos com iLO 4, mas não com iLO 2 ou iLO 3. Se for detectado um dispositivo com iLO 2 ou iLO, exclua-os manualmente na tela **Detalhes do dispositivo**.

# Verificar detecção

Para verificar se o P4000 foi detectado corretamente, siga estas instruções:

1. Se estiver sincronizando o Insight RS com o HP SIM, verifique se o Nome do dispositivo aparece corretamente na tela **Dispositivos**. Se o dispositivo aparecer como um número de série em vez de um endereço de IP ou nome de host, execute estas tarefas:
   a. Clique no nome do dispositivo e expanda a seção Status na guia **Dispositivo**. Clique em **Excluir dispositivo**.
   b. Na guia **Credenciais**, verifique se as credenciais associadas ao dispositivo estão corretas.
   c. Em **Configurações do administrador** → guia **Adaptadores de integração**, expanda a seção Adaptador do HP SIM e selecione **Realizar sincronização manual do dispositivo**.
   d. Clique na opção **Dispositivo único do HP SIM** e digite o endereço de IP ou nome do host do dispositivo P4000. Clique em **Salvar configurações do adaptador**.
2. Verifique se os protocolos apropriados foram atribuídos ao dispositivo P4000:
   a. No Insight RS Console, navegue até **Dispositivos** e clique no Nome do dispositivo P4000.
   b. Na guia Credenciais, verifique se os protocolos **P4000 SAN Solution (SAN/iQ)** e **SNMPv1** foram atribuídos ao dispositivo.

# Adicionar informações de garantia e contrato

Para adicionar as informações de garantia e de contrato do dispositivo P4000 ao Insight RS, conclua as seguintes etapas:

1. No Insight RS Console, navegue até **Dispositivos** e clique no Nome do dispositivo P4000.
2. Expanda a seção Hardware e digite o número de série no campo **Número de série substituto** e o número do produto no campo **Número do produto substituto**.
3. Clique em **Salvar alterações**.

# Verificar o status de detecção e do dispositivo

Para verificar se o dispositivo foi detectado corretamente, conclua as seguintes etapas:

1. Em um navegador da Web, faça logon no Insight RS Console.
2. No menu principal, selecione **Dispositivos** e clique na guia **Resumo do dispositivo**.
3. Verifique se a coluna Status contém um ícone de êxito ().

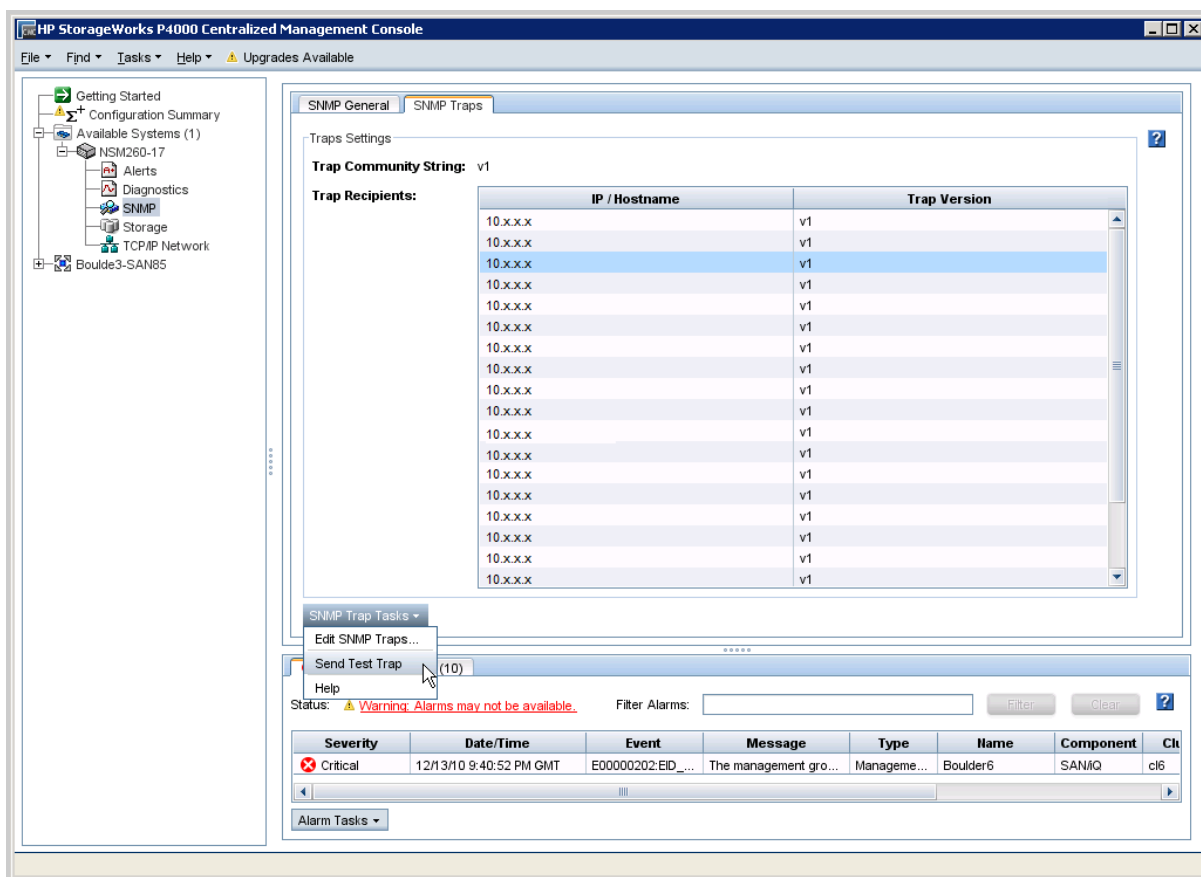
   Se não houver ícone de êxito, tente descobrir que coluna está com problema e consulte a Ajuda on-line para informações de solução de problemas.

# Verificar a comunicação entre o dispositivo monitorado e o Insight RS

Para verificar a comunicação entre o dispositivo monitorado e o Insight RS, conclua as seguintes seções:

## Enviar um evento de teste

Para verificar se os P4000 Storage Systems estão se comunicando com o dispositivo host, abra o CMC, selecione pelo menos um nó de armazenamento e envie uma interceptação de teste ao dispositivo host. Selecione **SNMP** na árvore de menu à esquerda e abra a guia **Armadilhas SNMP**. Na lista suspensa**Tarefas de armadilha SNMP**, selecione **Enviar armadilha de teste**.

**Observação:** No CMC, as armadilhas SNMP são configuradas no nível do grupo de gerenciamento, não no nível do nó.

Acesse as configurações do dispositivo host para verificar se o evento de teste foi registrado nos logs do dispositivo host. As credenciais de somente leitura do CMC foram verificadas durante a detecção do dispositivo quando cada dispositivo LeftHand OS foi adicionado ao dispositivo host monitorado listado.

# Verificar coletas no Insight RS Console

Coletas não são executadas automaticamente depois da descoberta. A HP recomenda que você execute uma coleta manualmente após a descoberta completa para verificar a conectividade. Execute o cronograma de coleta manualmente na guia Serviços de coleta → Agendamentos de coleta. Para obter mais informações sobre como agendar coletas, consulte a Ajuda do Insight RS.

Verifique se essa coleta foi bem-sucedida na guia Serviços de coleta → Resultados da coleta básica do Insight RS Console.

1. Faça logon no Insight RS Console.
2. No menu principal, selecione **Serviços de coleta** e depois clique na guia **Resultados da coleta básica**.
3. Expanda a seção Coleta de Configurações da Família P4000.
4. Localize a entrada referente ao seu dispositivo e verifique a coluna Resultado. Se a coleta tiver sido bem-sucedida, um ícone de êxito será exibido ( ). Se ocorrer uma falha, um ícone de erro será exibido ( ).

# Capítulo 22: Configurar Modular Smart Arrays P2000 G3, MSA 1040 e MSA 2040

## Atender aos requisitos de configuração

Para configurar Modular Smart Arrays P2000 G3, MSA 1040, e MSA 2040 de forma que elas sejam monitoradas pelo Insight RS, conclua as seguintes seções:

**Tabela 22.1** ***Etapas de configuração de Modular Smart Arrays P2000, MSA 1040 e MSA 2040***

| Tarefa | Concluída? |
|---|---|
| Verifique se o Insight RS oferece suporte ao seu Modular Smart Array, consultando o documento *Notas de Lançamento do HP Insight Remote Support*. | |
| Configure o SNMP no MSA. | |
| Configure o WBEM no MSA. | |
| Adicione o protocolo SNMP ao Insight RS Console. | |
| Adicione o protocolo WBEM ao Insight RS Console. | |
| Detecte o servidor Modular Smart Array no Insight RS Console. | |

## Instalar e configurar o software de comunicação em arrays

Para configurar seus dispositivos monitorados, conclua as seguintes seções:

## Configurar o SNMP em Modular Smart Arrays

Cada dispositivo MSA monitorado tem o SNMP já instalado de fábrica.

Para acessar o Storage Management Utility para o MSA e configurar o SNMP para o Insight Remote Support, conclua as seguintes etapas:

1. Faça logon no HP MSA Storage Management Utility (SMU).

**Observação:** Para obter informações básicas sobre como configurar essa ferramenta e gerenciar suas credenciais, consulte a documentação do MSA Storage Management Utility, em: http://www.hp.com/support/manuals.

2. Depois de entrar no utilitário, selecione **Configuração** → **Serviços** → **Gerenciamento**.
3. Certifique-se de selecionar o SNMP na lista **Serviços de gerenciamento de rede** e clique em **Aplicar**.

**Importante:** O SNMP deve ficar ativo por padrão. Porém, se por algum motivo ele não estiver, não haverá suporte para o Insight Remote Support. É extremamente importe

verificar se o SNMP está ativo.

4. No menu, selecione **Configuração** → **Serviços** → **Notificação SNMP**.
5. Na página **Configurar notificação SNMP**, modifique as configurações SNMP para incluir o dispositivo host como um host de interceptação de SNMP e selecione o **Nível de notificação** na lista suspensa (recomenda-se usar o nível Informativo).

6. Clique em **Aplicar** para as alterações terem efeito.
7. Saia do utilitário e detecte o MSA no Insight RS Console.

# Sobre o WBEM no P2000 G3, MSA 1040 e em MSA 2040 Modular Smart Arrays

O provedor SMI-S para o P2000 G3 MSA, o MSA 1040 e o MSA 2040 está integrado no firmware e é fornecido com matrizes de disco das séries P2000 G3, MSA 1040 e MSA 2040. Ele fornece uma estrutura de gerenciamento baseada no WBEM. O Insight RS pode interagir com esse provedor incorporado diretamente e não precisa de um provedor de proxy intermediário.

Nenhuma configuração do WBEM no P2000 G3, MSA 1040 e MSA 2040 é necessária.

# Definir configurações de firewall e porta

Para obter uma lista completa de requisitos de firewall e de porta para dispositivos monitorados, consulte o *Informe de Segurança do HP Insight Remote Support*, em: http://www.hp.com/go/insightremotesupport/docs.

# Adicionar credenciais de protocolo e iniciar a detecção

Para detectar seus dispositivos monitorados, conclua as seguintes seções:

# Criar uma credencial de protocolo SNMPv1 no Insight RS Console

Se a cadeia da comunidade SNMPv1 do dispositivo estiver definida como `pública` e o modo de acesso da comunidade for `somente leitura`, o Insight RS associará automaticamente um protocolo SNMP ao seu dispositivo. Se você usar uma cadeia de comunidade diferente ou uma porta não padrão, precisará criar uma credencial de protocolo SNMPv1 no Insight RS Console.

**Importante:** MSAs com o SNMPv3 habilitado exigem que credenciais SNMPv3 sejam configuradas no Insight RS Console. A falha em fornecer credenciais SNMPv3 no Insight RS Console faz com que o Insight RS mostre apenas um dos controladores desses MSAs.

Para configurar o SNMPv1 no Insight RS Console, conclua as seguintes etapas:

1. Em um navegador da Web, faça logon no Insight RS Console.
2. No menu principal, selecione **Detecção** e clique na guia **Credenciais**.
3. Na lista suspensa Selecionar e configurar protocolo, selecione **Simple Network Management Protocol versão 1 (SNMPv1)**.
4. Clique em **Novo**. A caixa de diálogo Nova credencial é exibida.
5. Digite a cadeia de caracteres da comunidade configurada no seu dispositivo.
6. Clique em **Adicionar**.

O Insight RS cria a credencial de protocolo, que é exibida na tabela de credenciais.

# Criar uma credencial de protocolo WBEM no Insight RS Console

Para configurar o WBEM no Insight RS Console, conclua as seguintes etapas:

1. Em um navegador da Web, faça logon no Insight RS Console.
2. No menu principal, selecione **Detecção** e clique na guia **Credenciais**.
3. Na lista suspensa **Selecionar e configurar protocolo**, selecione **Gerenciamento Corporativo baseado na Web (WBEM)**.
4. Clique em **Novo**. A caixa de diálogo Nova credencial é exibida.
5. Digite o nome de usuário e a senha usados para acessar a interface do Storage Management Utility no MSA.
6. Clique em **Adicionar**.

O Insight RS cria a credencial de protocolo, que é exibida na tabela de credenciais.

## Detectar o dispositivo no Insight RS Console

Para detectar o dispositivo por meio do Insight RS Console, conclua as seguintes etapas:

1. Em um navegador da Web, faça logon no Insight RS Console.
2. No menu principal, selecione **Detecção** e clique na guia **Fontes**.
3. Expanda a seção Endereços IP e adicione o endereço IP do seu dispositivo:
   a. Clique em **Novo**.
   b. Selecione **Endereço único**, **Intervalo de endereços** ou **Lista de endereços**.
   c. Digite os endereços IP dos dispositivos MSA a serem descobertos.

   **Importante:** Em um sistema de controlador duplo, você deve detectar tanto o controlador A quanto o controlador B, se ambos existirem. Se você não detectar ambos os controladores, talvez os eventos originados do controlador que não foi detectado sejam perdidos.

   d. Clique em **Adicionar**.
4. Clique em **Iniciar detecção**.

## Verificar o status de detecção e do dispositivo

Para verificar se o dispositivo foi detectado corretamente, conclua as seguintes etapas:

1. Em um navegador da Web, faça logon no Insight RS Console.
2. No menu principal, selecione **Dispositivos** e clique na guia **Resumo do dispositivo**.
3. Verifique se a coluna Status contém um ícone de êxito ().

   Se não houver ícone de êxito, tente descobrir que coluna está com problema e consulte a Ajuda on-line para informações de solução de problemas.

# Verificar a comunicação entre o dispositivo monitorado e o Insight RS

Para verificar a comunicação entre o dispositivo monitorado e o Insight RS, conclua as seguintes seções:

## Verificar o monitoramento de eventos de serviço

Para enviar um evento de teste do MSA, conclua as seguintes etapas:

1. Em um navegador da Web, faça logon no HP MSA Storage Management Utility (SMU).
2. Selecione **Ferramentas** → **Enviar notificação de teste**.

3. Na janela Enviar notificação de teste, clique em **Enviar**.
4. Clique em **OK** para confirmar que a mensagem foi enviada.
5. Saia do SMU.

# Verificar coletas no Insight RS Console

Coletas não são executadas automaticamente depois da descoberta. A HP recomenda que você execute uma coleta manualmente após a descoberta completa para verificar a conectividade. Execute o cronograma de coleta manualmente na guia Serviços de coleta → Agendamentos de coleta. Para obter mais informações sobre o agendamento de coletas, consulte a Ajuda do Insight RS.

Verifique se essa coleta foi bem-sucedida na guia Serviços de coleta → Resultados da Coleta de Armazenamento SAN no Insight RS Console.

1. Faça logon no Insight RS Console.
2. No menu principal, selecione **Serviços de coleta** e depois clique na guia **Resultados da Coleta de Armazenamento SAN**.
3. Expanda a seção Coleta de configurações de armazenamento.
4. Localize a entrada referente ao seu dispositivo e verifique a coluna Resultado. Se a coleta tiver sido bem-sucedida, um ícone de êxito será exibido (). Se ocorrer uma falha, um ícone de erro será exibido ().

# Capítulo 23: Configurar Modular Smart Arrays MSA23xx G2

## Atender aos requisitos de configuração

Para configurar arrays inteligentes modulares MSA23xx G2 de forma que eles sejam monitorados pelo Insight RS, conclua as seguintes seções:

**Tabela 23.1** ***Etapas de configuração de Modular Smart Arrays e P2000***

| Tarefa | Concluída? |
|---|---|
| Verifique se o Insight RS oferece suporte ao seu Modular Smart Array, consultando o documento *Notas de Lançamento do HP Insight Remote Support*. | |
| Configure o SNMP no MSA. | |
| Configure o WBEM no MSA. | |
| Adicione o protocolo SNMP ao Insight RS Console. | |
| Adicione o protocolo WBEM ao Insight RS Console. | |
| Detecte o servidor Modular Smart Array no Insight RS Console. | |

## Instalar e configurar o software de comunicação em arrays

Para configurar seus dispositivos monitorados, conclua as seguintes seções:

## Configurar o SNMP em MSA23xx G2 Modular Smart Arrays

Cada dispositivo MSA monitorado tem o SNMP já instalado de fábrica.

Para acessar o Storage Management Utility para o MSA23xx G2 e configurar o SNMP para o Insight Remote Support, conclua as seguintes etapas:

1. Faça logon no HP MSA Storage Management Utility.

**Observação:** Para obter informações básicas sobre como configurar essa ferramenta e gerenciar suas credenciais, consulte a documentação do MSA Storage Management Utility, em: http://www.hp.com/support/manuals.

2. Depois de entrar no utilitário, selecione **Configuração** → **Serviços** → **Gerenciamento**.
3. Certifique-se de selecionar o SNMP na lista **Serviços de gerenciamento de rede** e clique em **Aplicar**.

**Importante:** O SNMP deve ficar ativo por padrão. Porém, se por algum motivo ele não estiver, não haverá suporte para o Insight Remote Support. É extremamente importe

verificar se o SNMP está ativo.

4. No menu, selecione **Configuração** → **Serviços** → **Notificação SNMP**.
5. Na página **Configurar notificação SNMP**, modifique as configurações SNMP para incluir o dispositivo host como um host de interceptação de SNMP e selecione o **Nível de notificação** na lista suspensa (recomenda-se usar o nível Informativo).

6. Clique em **Aplicar** para as alterações terem efeito.
7. Saia do utilitário e detecte o 23xx no Insight RS Console.

# Instalar o software do provedor de proxy WBEM SMI-S

O software do provedor de proxy MSA2000 G2 SMI-S deve ser instalado em um servidor host ProLiant que irá gerenciar seus dispositivos MSA23xx. Ele fornece uma estrutura de gerenciamento baseada no WBEM. O Insight RS pode interagir com esse provedor de proxy para reunir coletas nos seus dispositivos MSA23xx.

Para baixar e instalar o software do provedor de proxy MSA2000 G2 SMI-S, conclua as seguintes etapas:

1. Em um navegador da Web, navegue até o seguinte site: http://www.hp.com/go/hpsc.
2. Na seção *Encontrar suporte para o seu produto HP*, digite sua família de produtos na caixa de pesquisa, por exemplo, MSA 2000 G2. Clique em **Ir**.
3. Selecione seu produto nos resultados da pesquisa.
4. Na seção *Drivers, softwares e firmwares para este produto*, clique no link **Visualizar e baixar todos os drivers, softwares e firmwares para este produto**.
5. Selecione seu produto e depois selecione o sistema operacional.
6. Na tabela *Downloads*, clique no link de software para o seu sistema operacional.

Para obter mais informações sobre como instalar e configurar o provedor de proxy SMI-S, consulte o *Guia do Usuário do Provedor de Proxy HP MSA2000 G2 SMI-S*.

# Definir configurações de firewall e porta

Para obter uma lista completa de requisitos de firewall e de porta para dispositivos monitorados, consulte o *Informe de Segurança do HP Insight Remote Support*, em: http://www.hp.com/go/insightremotesupport/docs.

# Adicionar credenciais de protocolo e iniciar a detecção

Para detectar seus dispositivos monitorados, conclua as seguintes seções:

## Criar uma credencial de protocolo SNMPv1 no Insight RS Console

Se a cadeia da comunidade SNMPv1 do dispositivo estiver definida como `pública` e o modo de acesso da comunidade for `somente leitura`, o Insight RS associará automaticamente um protocolo SNMP ao seu dispositivo. Se você usar uma cadeia de comunidade diferente ou uma porta não padrão, precisará criar uma credencial de protocolo SNMPv1 no Insight RS Console.

Para configurar o SNMPv1 no Insight RS Console, conclua as seguintes etapas:

1. Em um navegador da Web, faça logon no Insight RS Console.
2. No menu principal, selecione **Detecção** e clique na guia **Credenciais**.
3. Na lista suspensa Selecionar e configurar protocolo, selecione **Simple Network Management Protocol versão 1 (SNMPv1)**.
4. Clique em **Novo**. A caixa de diálogo Nova credencial é exibida.
5. Digite a cadeia de caracteres da comunidade configurada no seu dispositivo.
6. Clique em **Adicionar**.

O Insight RS cria a credencial de protocolo, que é exibida na tabela de credenciais.

## Criar uma credencial de protocolo WBEM no Insight RS

Para configurar o WBEM no Insight RS Console, conclua as seguintes etapas:

1. Em um navegador da Web, faça logon no Insight RS Console.
2. No menu principal, selecione **Detecção** e clique na guia **Credenciais**.
3. Na lista suspensa **Selecionar e configurar protocolo**, selecione **Gerenciamento Corporativo baseado na Web (WBEM)**.
4. Clique em **Novo**. A caixa de diálogo Nova credencial é exibida.
5. Digite o nome de usuário e a senha que você configurou para o MSA23xx no software do fornecedor de proxy SMI-S.
6. Clique em **Adicionar**.

O Insight RS cria a credencial de protocolo, que é exibida na tabela de credenciais.

## Detectar o dispositivo no Insight RS Console

Para detectar o dispositivo por meio do Insight RS Console, conclua as seguintes etapas:

1. Em um navegador da Web, faça logon no Insight RS Console.
2. No menu principal, selecione **Detecção** e clique na guia **Fontes**.
3. Expanda a seção Endereços IP e adicione o endereço IP a ser detectado.

   Ao detectar o MSA23xx G2, adicione o endereço IP de cada MSA23xx G2, juntamente com o servidor ProLiant que executa o software do provedor de proxy SMI-S. Isso garante que os serviços necessários de coleta e evento sejam configurados.

   a. Clique em **Novo**.
   b. Selecione **Endereço único**, **Intervalo de endereços** ou **Lista de endereços**.
   c. Digite os endereços IP do servidor ProLiant executando o software do provedor de proxy SMI-S e os dispositivos MSA23xx G2 a serem detectados.
   d. Clique em **Adicionar**.
4. Clique em **Iniciar detecção**.

## Verificar o status de detecção e do dispositivo

Para verificar se o dispositivo foi detectado corretamente, conclua as seguintes etapas:

1. Em um navegador da Web, faça logon no Insight RS Console.
2. No menu principal, selecione **Dispositivos** e clique na guia **Resumo do dispositivo**.
3. Verifique se a coluna Status contém um ícone de êxito ( ).

   Se não houver ícone de êxito, tente descobrir que coluna está com problema e consulte a Ajuda on-line para informações de solução de problemas.

# Verificar a comunicação entre o dispositivo monitorado e o Insight RS

Para verificar a comunicação entre o dispositivo monitorado e o Insight RS, conclua a seguinte seção:

## Verificar coletas no Insight RS Console

Coletas não são executadas automaticamente depois da descoberta. A HP recomenda que você execute uma coleta manualmente após a descoberta completa para verificar a conectividade. Execute o cronograma de coleta manualmente na guia Serviços de coleta → Agendamentos de coleta. Para obter mais informações sobre o agendamento de coletas, consulte a Ajuda do Insight RS.

Verifique se essa coleta foi bem-sucedida na guia Serviços de coleta → Resultados da Coleta de Armazenamento SAN no Insight RS Console.

1. Faça logon no Insight RS Console.
2. No menu principal, selecione **Serviços de coleta** e depois clique na guia **Resultados da Coleta de Armazenamento SAN**.
3. Expanda a seção Coleta de configurações de armazenamento.
4. Localize a entrada referente ao seu dispositivo e verifique a coluna Resultado. Se a coleta tiver sido bem-sucedida, um ícone de êxito será exibido ( ). Se ocorrer uma falha, um ícone de erro será exibido ( ).

# Capítulo 24: Configurar Modular Smart Arrays MSA2xxx G1

**Importante:** Não há suporte para coletas de configuração, exceto quando o MSA2xxx G1 faz parte de uma coleta de SAN.

## Atender aos requisitos de configuração

Para configurar arrays inteligentes modulares MSA2xxx G1 de forma que eles sejam monitorados pelo Insight RS, conclua as seguintes seções:

**Tabela 24.1** ***Etapas de configuração de Modular Smart Arrays e P2000***

| Tarefa | Concluída? |
|---|---|
| Verifique se o Insight RS oferece suporte ao seu Modular Smart Array, consultando o documento *Notas de Lançamento do HP Insight Remote Support*. | |
| Configure o SNMP no MSA. | |
| Adicione o protocolo SNMP ao Insight RS Console. | |
| Detecte o servidor Modular Smart Array no Insight RS Console. | |

## Instalar e configurar o software de comunicação em arrays

Para configurar seus dispositivos monitorados, conclua as seguintes seções:

## Configurar o SNMP em MSA2xxx G1 Modular Smart Arrays

Cada dispositivo MSA monitorado tem o SNMP já instalado de fábrica.

Para acessar o Storage Management Utility para o MSA 2012 ou 2112 e configurar o SNMP para o Insight Remote Support, conclua as seguintes etapas:

1. Faça logon no HP MSA Storage Management Utility.

**Observação:** Para obter informações básicas sobre como configurar essa ferramenta e gerenciar suas credenciais, consulte a documentação do MSA Storage Management Utility, em: http://www.hp.com/support/manuals.

2. Selecione **Gerenciar**.

3. Na lista expandida, selecione o link **Notificação de eventos**.

4. Na página **Resumo da notificação de eventos**, verifique se os tipos de notificação SNMP estão ativados (alertas visuais, alertas por e-mail e interceptações de SNMP), depois clique em **Alterar configurações de notificação**.

5. Clique no link **Configuração de SNMP** abaixo do título Notificação de eventos no painel esquerdo.
6. Modifique as configurações de SNMP para incluir o dispositivo host como um Host de interceptação de SNMP e certifique-se de que a opção **Interceptações de SNMP habilitadas** esteja marcada como **Sim**.

7. Clique em **Alterar configurações de interceptações de SNMP** para aplicar as mudanças.

**Observação:** Se o dispositivo host do Insight Remote Support estiver totalmente configurado, você poderá enviar o evento de teste dessa página. Se o dispositivo host ainda não estiver configurado, você pode voltar a esta página mais tarde e enviar o evento de teste.

8. Saia do utilitário e detecte o 2012/2112 no Insight RS Console.

# Definir configurações de firewall e porta

Para obter uma lista completa de requisitos de firewall e de porta para dispositivos monitorados, consulte o *Informe de Segurança do HP Insight Remote Support*, em: http://www.hp.com/go/insightremotesupport/docs.

# Adicionar credenciais de protocolo e iniciar a detecção

Para detectar seus dispositivos monitorados, conclua as seguintes seções:

# Criar uma credencial de protocolo SNMPv1 no Insight RS Console

Se a cadeia da comunidade SNMPv1 do dispositivo estiver definida como `pública` e o modo de acesso da comunidade for `somente leitura`, o Insight RS associará automaticamente um protocolo SNMP ao seu dispositivo. Se você usar uma cadeia de comunidade diferente ou uma porta não padrão, precisará criar uma credencial de protocolo SNMPv1 no Insight RS Console.

Para configurar o SNMPv1 no Insight RS Console, conclua as seguintes etapas:

1. Em um navegador da Web, faça logon no Insight RS Console.
2. No menu principal, selecione **Detecção** e clique na guia **Credenciais**.
3. Na lista suspensa Selecionar e configurar protocolo, selecione **Simple Network Management Protocol versão 1 (SNMPv1)**.
4. Clique em **Novo**. A caixa de diálogo Nova credencial é exibida.
5. Digite a cadeia de caracteres da comunidade configurada no seu dispositivo.
6. Clique em **Adicionar**.

O Insight RS cria a credencial de protocolo, que é exibida na tabela de credenciais.

## Detectar o dispositivo no Insight RS Console

Para detectar o dispositivo por meio do Insight RS Console, conclua as seguintes etapas:

1. Em um navegador da Web, faça logon no Insight RS Console.
2. No menu principal, selecione **Detecção** e clique na guia **Fontes**.
3. Expanda a seção Endereços IP e adicione o endereço IP do seu dispositivo:
   a. Clique em **Novo**.
   b. Selecione **Endereço único**, **Intervalo de endereços** ou **Lista de endereços**.
   c. Digite os endereços IP dos dispositivos a serem detectados.
   d. Clique em **Adicionar**.
4. Clique em **Iniciar detecção**.

## Verificar o status de detecção e do dispositivo

Para verificar se o dispositivo foi detectado corretamente, conclua as seguintes etapas:

1. Em um navegador da Web, faça logon no Insight RS Console.
2. No menu principal, selecione **Dispositivos** e clique na guia **Resumo do dispositivo**.
3. Verifique se a coluna Status contém um ícone de êxito ( ).

   Se não houver ícone de êxito, tente descobrir que coluna está com problema e consulte a Ajuda on-line para informações de solução de problemas.

# Verificar a comunicação entre o dispositivo monitorado e o Insight RS

Para verificar a comunicação entre o dispositivo monitorado e o Insight RS, conclua a seguinte seção:

# Verificar coletas no Insight RS Console

Coletas de configuração não têm suporte para esse tipo de dispositivo, exceto quando ele faz parte de uma coleta de SAN. Se você adicionou esse dispositivo a uma coleta de SAN, poderá executar manualmente uma coleta de SAN para verificar a configuração.

1. Faça logon no Insight RS Console.
2. No menu principal, selecione **Serviços de coleta**.
3. Clique na guia **Agendamentos de coleta**.
4. No painel Lista de agendamentos de coleta, selecione **Agendamento de coletas de configuração da SAN**. Informações sobre a coleta são exibidas no painel Informações da coleta. O painel Nestes dispositivos lista os dispositivos em que a coleta será executada.
5. No painel Informações de agendamento, clique em **Executar agora**.
6. Quando a coleta terminar, clique na guia **Resultados da Coleta de Armazenamento SAN**.
7. Expanda a seção Coleta de Configurações de SAN.
8. Localize a entrada referente ao seu dispositivo e verifique a coluna Resultado. Se a coleta tiver sido bem-sucedida, um ícone de êxito será exibido ( ). Se ocorrer uma falha, um ícone de erro será exibido ( ).

# Capítulo 25: Configurar Modular Smart Arrays MSA15xx

## Atender aos requisitos de configuração

Para configurar matrizes inteligentes modulares MSA15xx de forma que elas sejam monitoradas pelo Insight RS, conclua as seguintes seções:

**Tabela 25.1** ***Etapas de configuração de Modular Smart Arrays e P2000***

| Tarefa | Concluída? |
|---|---|
| Verifique se o Insight RS oferece suporte ao seu Modular Smart Array, consultando o documento *Notas de Lançamento do HP Insight Remote Support*. | |
| Configure o SNMP no MSA. | |
| Adicione o protocolo SNMP ao Insight RS Console. | |
| Detecte o servidor Modular Smart Array no Insight RS Console. | |

## Instalar e configurar o software de comunicação em arrays

Para configurar seus dispositivos monitorados, conclua as seguintes seções:

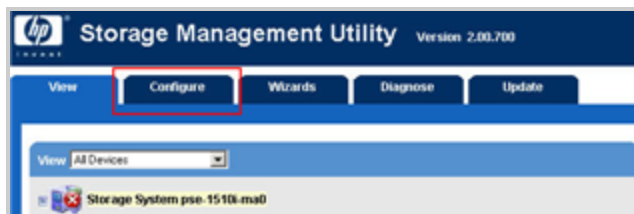
## Configurar o SNMP em arrays MSA15xx Modular Smart Arrays

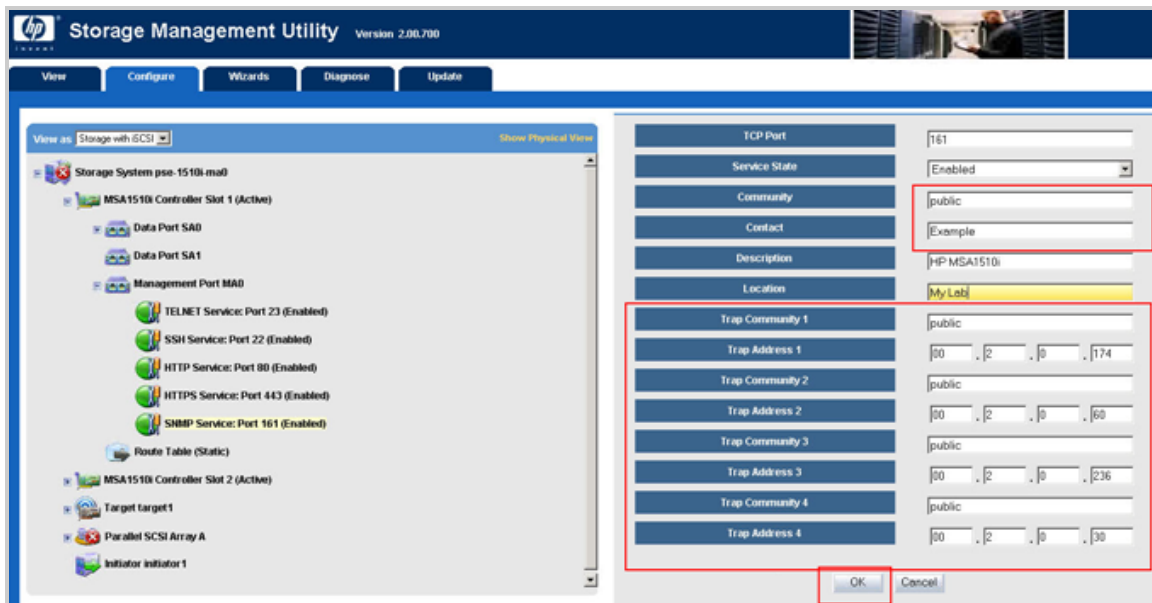
Cada dispositivo MSA monitorado tem o SNMP já instalado de fábrica.

Para acessar o Storage Management Utility para o MSA 1510i e configurar o SNMP para o Insight Remote Support, conclua as seguintes etapas:

1. Faça logon no HP MSA Storage Management Utility.

**Observação:** Para obter informações básicas sobre como configurar essa ferramenta e gerenciar suas credenciais, consulte a documentação do MSA Storage Management Utility, em: http://www.hp.com/support/manuals.

2. Depois de entrar no utilitário, selecione a guia **Configurar**.

3. Na guia **Configurar**, expanda a lista **Porta de gerenciamento** para o MSA 1510i.
4. Selecione o link **Serviço SNMP** na lista.

5. Modifique os campos de configuração necessários e certifique-se de que o endereço de IP do dispositivo host esteja listado como **Endereço de interceptação**.
6. Clique em **OK** para aplicar as alterações.

7. Saia do utilitário e detecte o 1510i no Insight RS Console.

# Definir configurações de firewall e porta

Para obter uma lista completa de requisitos de firewall e de porta para dispositivos monitorados, consulte

o *Informe de Segurança do HP Insight Remote Support*, em:
http://www.hp.com/go/insightremotesupport/docs.

# Adicionar credenciais de protocolo e iniciar a detecção

Para detectar seus dispositivos monitorados, conclua as seguintes seções:

## Criar uma credencial de protocolo SNMPv1 no Insight RS Console

Se a cadeia da comunidade SNMPv1 do dispositivo estiver definida como `pública` e o modo de acesso da comunidade for `somente leitura`, o Insight RS associará automaticamente um protocolo SNMP ao seu dispositivo. Se você usar uma cadeia de comunidade diferente ou uma porta não padrão, precisará criar uma credencial de protocolo SNMPv1 no Insight RS Console.

Para configurar o SNMPv1 no Insight RS Console, conclua as seguintes etapas:

1. Em um navegador da Web, faça logon no Insight RS Console.
2. No menu principal, selecione **Detecção** e clique na guia **Credenciais**.
3. Na lista suspensa Selecionar e configurar protocolo, selecione **Simple Network Management Protocol versão 1 (SNMPv1)**.
4. Clique em **Novo**. A caixa de diálogo Nova credencial é exibida.
5. Digite a cadeia de caracteres da comunidade configurada no seu dispositivo.
6. Clique em **Adicionar**.

O Insight RS cria a credencial de protocolo, que é exibida na tabela de credenciais.

## Detectar o dispositivo no Insight RS Console

Para detectar o dispositivo por meio do Insight RS Console, conclua as seguintes etapas:

1. Em um navegador da Web, faça logon no Insight RS Console.
2. No menu principal, selecione **Detecção** e clique na guia **Fontes**.
3. Expanda a seção Endereços IP e adicione o endereço IP do seu dispositivo:
   a. Clique em **Novo**.
   b. Selecione **Endereço único**, **Intervalo de endereços** ou **Lista de endereços**.
   c. Digite os endereços IP dos dispositivos a serem detectados.
   d. Clique em **Adicionar**.
4. Clique em **Iniciar detecção**.

## Verificar o status de detecção e do dispositivo

Para verificar se o dispositivo foi detectado corretamente, conclua as seguintes etapas:

1. Em um navegador da Web, faça logon no Insight RS Console.
2. No menu principal, selecione **Dispositivos** e clique na guia **Resumo do dispositivo**.
3. Verifique se a coluna Status contém um ícone de êxito ().

   Se não houver ícone de êxito, tente descobrir que coluna está com problema e consulte a Ajuda on-line para informações de solução de problemas.

# Verificar a comunicação entre o dispositivo monitorado e o Insight RS

Para verificar a comunicação entre o dispositivo monitorado e o Insight RS, conclua a seguinte seção:

## Verificar coletas no Insight RS Console

Coletas não são executadas automaticamente depois da descoberta. A HP recomenda que você execute uma coleta manualmente após a descoberta completa para verificar a conectividade. Execute o cronograma de coleta manualmente na guia Serviços de coleta → Agendamentos de coleta. Para obter mais informações sobre o agendamento de coletas, consulte a Ajuda do Insight RS.

Verifique se essa coleta foi bem-sucedida na guia Serviços de coleta → Resultados da Coleta de Armazenamento SAN no Insight RS Console.

1. Faça logon no Insight RS Console.
2. No menu principal, selecione **Serviços de coleta** e depois clique na guia **Resultados da Coleta de Armazenamento SAN**.
3. Expanda a seção Coleta de configurações de armazenamento.
4. Localize a entrada referente ao seu dispositivo e verifique a coluna Resultado. Se a coleta tiver sido bem-sucedida, um ícone de êxito será exibido (). Se ocorrer uma falha, um ícone de erro será exibido ().

# Capítulo 26: Configurar sistemas StoreEasy Storage

O Insight Remote Support (RS) requer que o WMI esteja instalado e configurado no seu sistema StoreEasy Storage (o antigo Network Storage Systems) para que o Insight RS se comunique com o seu dispositivo para detecção, monitoramento de eventos e coletas.

O WMI vem pré-instalado em sistemas StoreEasy Storage. Nenhuma configuração adicional do WMI é necessária. No entanto, é necessário adicionar as credenciais do protocolo WMI no Insight RS Console para que o Insight RS possa se comunicar com o seu dispositivo.

## Atender aos requisitos de configuração

Para configurar seu sistema StoreEasy Storage de forma que ele seja monitorado pelo Insight RS, conclua as seguintes seções:

**Tabela 26.1** ***Etapas da configuração do sistema StoreEasy Storage***

| Tarefa | Concluída? |
|---|---|
| Consulte as *Notas de Lançamento do HP Insight Remote Support* para garantir que haja suporte para o seu sistema de armazenamento StoreEasy. | |
| Adicione o protocolo WMI ao Insight RS Console. | |
| Detecte o sistema StoreEasy Storage no Insight RS Console. | |
| Envie um evento de teste para verificar a conectividade entre seu sistema StoreEasy Storage e o Insight RS. | |

## Configurar dispositivos StoreEasy

Para configurar seus dispositivos monitorados, conclua a seguinte seção:

## Configurar o firewall

Dispositivos StoreEasy são fornecidos com o recurso Firewall do Windows com Segurança Avançada habilitado. Para permitir o WMI através do Firewall do Windows, você deverá habilitar regras adicionais de entrada e saída.

Para configurar o Firewall do Windows no dispositivo StoreEasy, conclua as seguintes etapas:

1. Abra o Firewall do Windows a partir do Gerenciador de servidores.
2. Clique no menu **Ferramentas**.
3. Selecione **Firewall do Windows com Segurança Avançada**.
4. Selecione o link **Regras de entrada** no menu esquerdo e verifique se as seguintes regras de entrada estão habilitadas:
   - Compartilhamento de arquivos e impressora (Solicitação de eco - ICMPv4-Entrada)
   - Windows Management Instrumentation (DCOM-In)

- Windows Management Instrumentation (WMI-In)

5. Selecione o link **Regras de saída** no menu esquerdo e verifique se as seguintes regras de saída estão habilitadas:
   - Compartilhamento de arquivos e impressora (Solicitação de eco - ICMPv4-Saída)
   - Windows Management Instrumentation (WMI-Out)

Mais informações sobre segurança no Insight RS podem ser encontradas no *Informe de Segurança do HP Insight Remote Support*, em: http://www.hp.com/go/insightremotesupport/docs.

**Observação:** Você pode confirmar qual detecção de protocolos está associada ao dispositivo StoreEasy clicando no nome desse dispositivo na tela **Dispositivos** e selecionando a guia **Credenciais**. Confirme se o WMI é uma das credenciais descobertas. O SNMP não deve estar entre as credenciais detectadas.

# Adicionar credenciais de protocolo e iniciar a detecção

Para detectar seus dispositivos monitorados, conclua as seguintes seções:

## Criar uma credencial de protocolo WMI no Insight RS Console

Credenciais do WMI devem ser definidas para cada sistema StoreEasy Storage no Insight RS Console antes que ele possa ser monitorado. Se você alterar suas credenciais do WMI a qualquer momento, *deverá* modificar a entrada dessas credenciais no Insight RS Console.

Para configurar o WMI no Insight RS Console, conclua as seguintes etapas:

1. Em um navegador da Web, faça logon no Insight RS Console.
2. No menu principal, selecione **Detecção** e clique na guia **Credenciais**.
3. Na lista suspensa **Selecionar e configurar protocolo**, selecione **Instrumentação de Gerenciamento do Windows (WMI)**.
4. Clique em **Novo**. A caixa de diálogo Nova credencial é exibida.
5. Digite o nome de usuário e a senha configurados no seu dispositivo.
6. Clique em **Adicionar**.

O Insight RS cria a credencial de protocolo, que é exibida na tabela de credenciais.

## Detectar o dispositivo no Insight RS Console

Para detectar o dispositivo por meio do Insight RS Console, conclua as seguintes etapas:

1. Em um navegador da Web, faça logon no Insight RS Console.
2. No menu principal, selecione **Detecção** e clique na guia **Fontes**.

3. Expanda a seção Endereços IP e adicione o endereço IP do seu dispositivo:
   a. Clique em **Novo**.
   b. Selecione **Endereço único**, **Intervalo de endereços** ou **Lista de endereços**.
   c. Digite os endereços IP dos dispositivos a serem detectados.
   d. Clique em **Adicionar**.
4. Clique em **Iniciar detecção**.

# Verificar o status de detecção e do dispositivo

Para verificar se o dispositivo foi detectado corretamente, conclua as seguintes etapas:

1. Em um navegador da Web, faça logon no Insight RS Console.
2. No menu principal, selecione **Dispositivos** e clique na guia **Resumo do dispositivo**.
3. Verifique se a coluna Status contém um ícone de êxito (✅).

   Se não houver ícone de êxito, tente descobrir que coluna está com problema e consulte a Ajuda on-line para informações de solução de problemas.

# Verificar a comunicação entre o dispositivo monitorado e o Insight RS

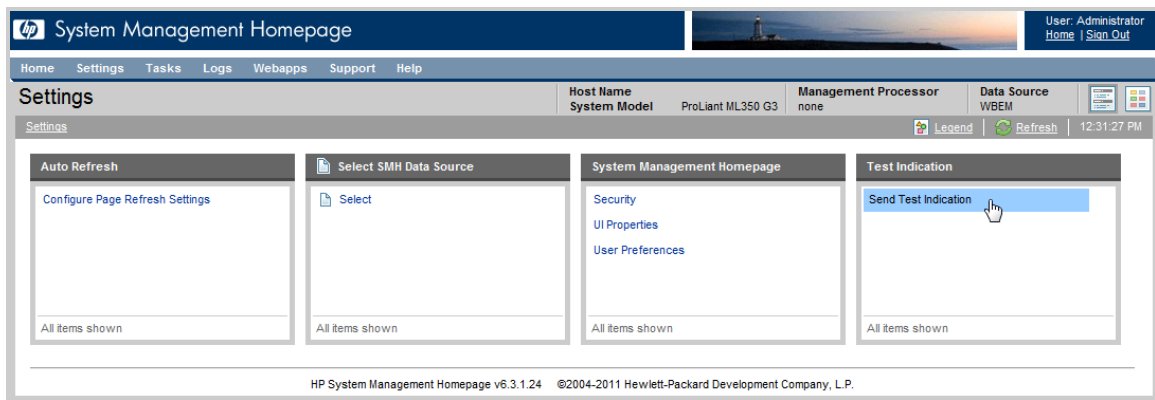
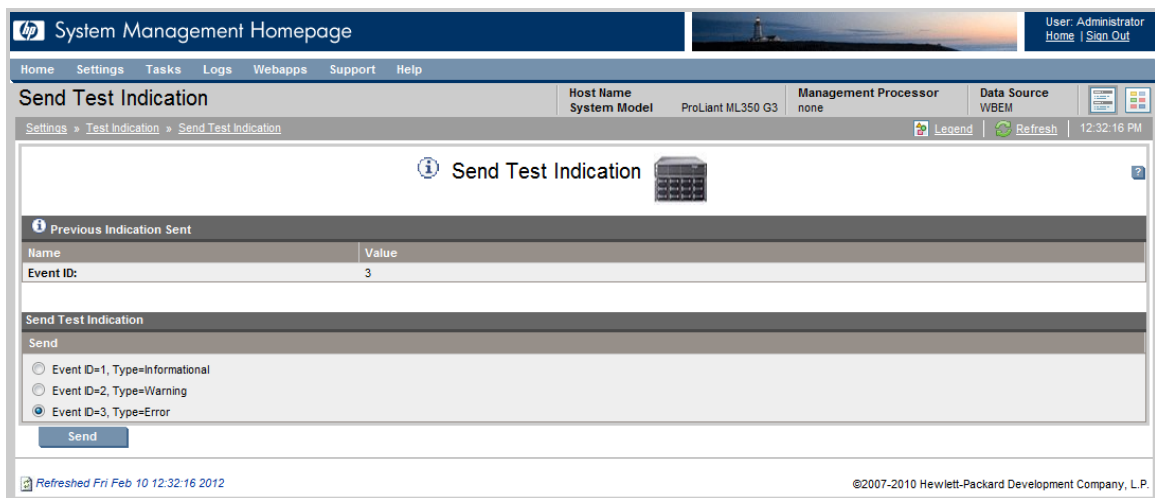
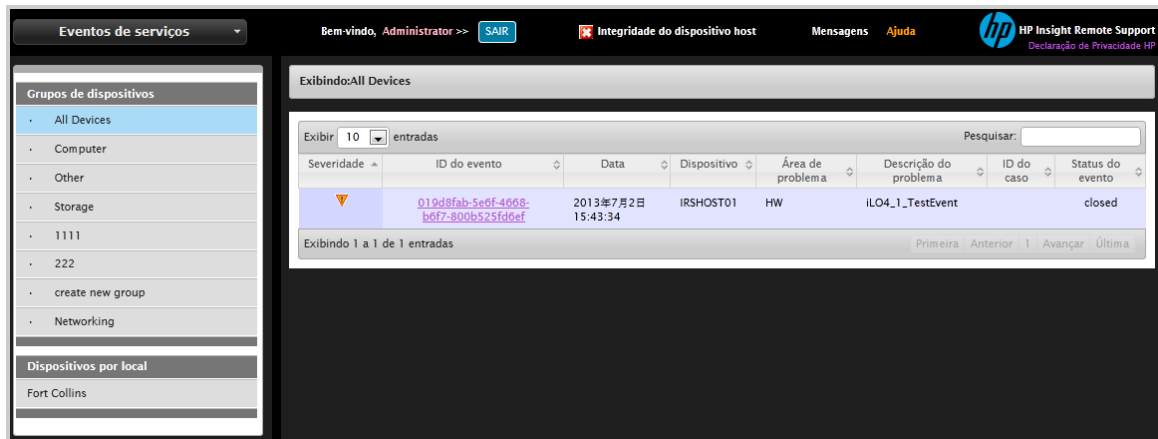
Para verificar a comunicação entre o dispositivo monitorado e o Insight RS, conclua as seguintes seções:

# Enviar uma indicação de teste do WMI ao dispositivo host

O System Management Homepage (SMH) também vem pré-instalado no seu sistema StoreEasy Storage. Ela fornece recursos adicionais de geração de relatórios no próprio dispositivo. Mesmo que não seja obrigatório para o Insight Remote Support, o SMH pode ser usado para operar com o protocolo WMI, por exemplo, para enviar eventos de teste.

Para verificar a conexão do dispositivo com o Insight RS, envie uma indicação de teste WMI ao dispositivo host e verifique se o teste de interceptação foi recebido no Insight RS Console.

1. Em um navegador, acesse o System Management Homepage (SMH) no dispositivo monitorado: `https://[`*`endereçoIP`*`]:2381`.
2. Faça login usando o nome do usuário administrador e a senha do dispositivo monitorado.

   se não aparecer a tela de login, clique no link **Entrar** no canto superior direito da interface da SMH. Se você não estiver conectado como administrador do dispositivo monitorado, não terá todas as opções de configuração relevantes.
3. Na barra superior do menu, clique em **Configurações**.
4. Se você tiver optado pela instalação de WMI com o SPP, ele será definido como sua fonte de dados. No painel Indicação de teste, clique em **Enviar indicação de teste**.

5. Na tela **Enviar indicação de teste**, selecione um tipo de ID de evento (pode ser qualquer uma) e clique em **Enviar**.

# Visualizar eventos de teste no Insight RS Console

Depois de enviar a indicação de teste, verifique se ela chegou no Insight RS Console.

Para verificar se a indicação de teste chegou, conclua as seguintes etapas:

1. Em um navegador da Web, faça logon no Insight RS Console.
2. No menu principal, selecione **Eventos de serviços**. Se o dispositivo monitorado estiver configurado

adequadamente, o evento aparecerá no painel Informações sobre eventos de serviços.

# Verificar coletas

Coletas não são executadas automaticamente depois da descoberta. A HP recomenda que você execute uma coleta manualmente após a descoberta completa para verificar a conectividade. Execute o cronograma de coleta manualmente na guia Serviços de coleta → Agendamentos de coleta. Para obter mais informações sobre como agendar coletas, consulte a Ajuda do Insight RS.

Observe também que os sistemas StoreEasy Storage usam coletas de configurações básicas do servidor no lugar de coletas de configurações de armazenamento.

Verifique se essa coleta foi bem-sucedida na guia Serviços de coleta → Resultados da coleta básica do Insight RS Console.

1. Faça logon no Insight RS Console.
2. No menu principal, selecione **Serviços de coleta** e depois clique na guia **Resultados da coleta básica**.
3. Expanda a seção Coleta de configurações básicas do servidor.
4. Localize a entrada referente ao seu dispositivo e verifique a coluna Resultado. Se a coleta tiver sido bem-sucedida, um ícone de êxito será exibido (). Se ocorrer uma falha, um ícone de erro será exibido ().

# Capítulo 27: Configurar sistemas StoreAll Storage

**Observação:** HP StoreAll Storage é o novo nome do HP IBRIX Storage.

Observe as seguintes limitações:

- Para sistemas X9000, a implementação do Insight Remote Support fica limitada a eventos de hardware.
- Em algumas configurações manuais, os nós X9320 e X9300 precisam ser reconhecidos como uma solução X9000. Consulte a seção "Configurar informações de garantia e contrato".

## Atender aos requisitos de configuração

Para configurar seus sistemas de armazenamento de forma que eles sejam monitorados pelo Insight RS, conclua as seguintes seções:

**Tabela 27.1** ***Etapas da configuração do sistema StoreAll Storage***

| Tarefa | Concluída? |
|---|---|
| Certifique-se de que o Insight RS oferece suporte ao seu sistema StoreAll Storage, verificando o documento *Notas de Lançamento do HP Insight Remote Support*. | |
| Configure o SNMP nos nós do servidor de arquivo. | |
| Reinicie os agentes do Insight Management. | |
| Adicione o protocolo SNMP ao Insight RS Console. | |
| Detecte o sistema StoreAll Storage no Insight RS Console. | |
| Configure informações de garantia e contrato no Insight RS Console. | |
| Envie um evento de teste para verificar a conectividade entre seu sistema StoreAll Storage e o Insight RS. | |

## Instalar e configurar o software de comunicação em sistemas de armazenamento

Para configurar seus dispositivos monitorados, conclua as seguintes seções:

## Configurar o SNMP nos nós de servidor de arquivos

1. Execute o script `/sbin/hpsnmpconfig`, que configura o SNMP para integrar o dispositivo host sendo executado no servidor Windows com a Página inicial do gerenciamento de sistemas HP no nó de servidor de arquivos. O script edita o arquivo `/etc/snmp/snmpd.conf`, acrescentando entradas parecidas com as seguintes:

```
# Following entries were added by HP Insight Management Agents at
# <data> <hora> UTC <ano>
dlmod cmaX /usr/lib64/libcmaX64.so
rwcommunity public 127.0.0.1
rocommunity public 127.0.0.1
rwcommunity public <IP do gerente>
rocommunity public <IP do gerente>
trapcommunity public
trapsink <IP do gerente> public
syscontact
syslocation
# ---------------------- FIM --------------------
```

2. Para adicionar mais de um IP de gerente SNMP, copie as seguintes linhas:

```
rwcommunity public <IP do gerente>
rocommunity public <IP do gerente>
trapsink <IP do gerente> public
```

3. Depois de atualizar o arquivo snmpd.conf, reinicie o serviço snmp:

```
# service snmpd restart
```

Para mais informações sobre o script `/sbin/hpsnmpconfig`, consulte “Configuração SNMP” na página principal de hp-snmp-agents(4). Para informações sobre a Página inicial do gerenciamento de sistemas HP, acesse: http://h18013.www1.hp.com/products/servers/management/agents/index.html.

**Importante:** O arquivo `/opt/hp/hp-snmp-agents/cma.conf` controla determinadas ações nos agentes SNMP. Você pode acrescentar uma entrada trapIf ao arquivo para configurar o endereço de IP usado pelo daemon SNMP quando for enviar interceptações. Por exemplo, para enviar interceptações usando o endereço de IP da interface eth1, acrescente o seguinte:

trapIf eth1

Depois reinicie os agentes HP SNMP:

service hp-snmp-agents restart

Para mais informações sobre o arquivo `cma.conf`, consulte a seção 3.1 de *Manual de gerenciamento de servidores ProLiant com Linux*: http://h20000.www2.hp.com/bc/docs/support/SupportManual/c00223285/c00223285.pdf.

# Iniciar ou reiniciar agentes do Insight Management

No X9000, inicie ou reinicie os seguintes serviços:

- Página inicial do gerenciamento de sistemas:

  ```
  # service hpsmhd restart
  ```

- Agente SNMP:

  ```
  # service snmpd restart
  ```

- Agentes HP SNMP:

  ```
  # service hp-snmp-agents start
  ```

  Para garantir que `hp-snmp-agents` se reinicie quando o sistema for reinicializado, digite o seguinte comando:

  ```
  # chkconfig hp-snmp-agents on
  ```

# Adicionar credenciais de protocolo e iniciar a detecção

Para detectar seus dispositivos monitorados, conclua as seguintes seções:

## Criar uma credencial de protocolo SNMPv1 no Insight RS Console

Se a cadeia da comunidade SNMPv1 do dispositivo estiver definida como `pública` e o modo de acesso da comunidade for `somente leitura`, o Insight RS associará automaticamente um protocolo SNMP ao seu dispositivo. Se você usar uma cadeia de comunidade diferente ou uma porta não padrão, precisará criar uma credencial de protocolo SNMPv1 no Insight RS Console.

Para configurar o SNMPv1 no Insight RS Console, conclua as seguintes etapas:

1. Em um navegador da Web, faça logon no Insight RS Console.
2. No menu principal, selecione **Detecção** e clique na guia **Credenciais**.
3. Na lista suspensa Selecionar e configurar protocolo, selecione **Simple Network Management Protocol versão 1 (SNMPv1)**.
4. Clique em **Novo**. A caixa de diálogo Nova credencial é exibida.
5. Digite a cadeia de caracteres da comunidade configurada no seu dispositivo.
6. Clique em **Adicionar**.

O Insight RS cria a credencial de protocolo, que é exibida na tabela de credenciais.

## Detectar o dispositivo no Insight RS Console

Para detectar o dispositivo por meio do Insight RS Console, conclua as seguintes etapas:

1. Em um navegador da Web, faça logon no Insight RS Console.
2. No menu principal, selecione **Detecção** e clique na guia **Fontes**.
3. Expanda a seção Endereços IP e adicione o endereço IP do seu dispositivo:

a. Clique em **Novo**.
   b. Selecione **Endereço único**, **Intervalo de endereços** ou **Lista de endereços**.
   c. Digite os endereços IP dos dispositivos a serem detectados.
   d. Clique em **Adicionar**.
4. Clique em **Iniciar detecção**.

# Configurar informações de garantia e contrato

Configure o Insight RS Console para habilitar suporte remoto para sistemas X9000.

- **Configurações personalizadas de campo para X9300/X9320**

  Os servidores são detectados com os respectivos endereços de IP. Quando um servidor for detectado, edite as propriedades do sistema no Insight RS Console. No menu principal, clique em **Dispositivos** e, em seguida, clique no nome de dispositivo do seu sistema.

  Na guia Dispositivos, na seção Hardware:

  - Insira o número do produto do gabinete X9000 como o Número de produto substituto
  - Insira `MC DATACENTER` ou `MC HYPERSCALE` como a ID de entrega personalizada

  Na guia Dispositivo, na seção Garantia e contrato:

  - Digite o Tipo de suporte e o Identificador de suporte apropriados

- **Configurações de campo personalizadas para o MSA Storage Management Utility**

  Defina as configurações SNMP na seção MSA Storage Management Utility. (Para mais informações, consulte "Configurar notificação de evento SNMP em SMU", no *Guia de referência da matriz inteligente modular 2300*. http://www.hp.com/support/manuals. Na página Manuais, selecione **Armazenamento** → **Sistemas de armazenamento em disco** → **Matrizes de disco MSA** → **HP 2000sa G2 Modular Smart Array** ou **HP P2000 G3 MSA Array Systems**.)

  Uma unidade de matriz de armazenamento modular (MSA) deve ser detectada com esse endereço de IP. Depois da detecção, localize a seção Informações de direito, na página Informações de garantia e do contrato, para atualizar o seguinte:

  - Insira `MC DATACENTER` ou `MC HYPERSCALE` como a ID de entrega personalizada
  - Digite o Tipo de suporte e o Identificador de suporte apropriados

**Observação:** Para suporte de armazenamento em sistemas X 9300, não defina a ID de entrega personalizada:. (O MSA é uma exceção; a ID de entrega personalizada é definida conforme descrito anteriormente.)

# Verificar o status de detecção e do dispositivo

Para verificar se o dispositivo foi detectado corretamente, conclua as seguintes etapas:

1. Em um navegador da Web, faça logon no Insight RS Console.
2. No menu principal, selecione **Dispositivos** e clique na guia **Resumo do dispositivo**.

3. Verifique se a coluna Status contém um ícone de êxito ().

   Se não houver ícone de êxito, tente descobrir que coluna está com problema e consulte a Ajuda on-line para informações de solução de problemas.

# Verificar a comunicação entre o dispositivo monitorado e o Insight RS

Para verificar a comunicação entre o dispositivo monitorado e o Insight RS, conclua as seguintes seções:

## Enviar uma interceptação de teste

Para conferir se as interceptações estão funcionando corretamente, envie uma interceptação genérica de teste com o seguinte comando:

```
snmptrap -v1 -c public <IP do dispositivo host> .1.3.6.1.4.1.232 <IP do sistema
gerenciado> 6 11003 1234 .1.3.6.1.2.1.1.5.0 s test .1.3.6.1.4.1.232.11.2.11.1.0 i 0
.1.3.6.1.4.1.232.11.2.8.1.0 s "X9000 remote support testing"
```

Por exemplo, se o endereço de IP do dispositivo host for 10.2.2.2 e o nó X9000 for 10.2.2.10, digite o seguinte:

```
snmptrap -v1 -c public 10.2.2.2 .1.3.6.1.4.1.232 10.2.2.10 6 11003 1234
.1.3.6.1.2.1.1.5.0 s test .1.3.6.1.4.1.232.11.2.11.1.0 i 0 .1.3.6.1.4.1.232.11.2.8.1.0
s "X9000 remote support testing"
```

Para o Insight Remote Support, substitua o endereço IP do dispositivo host pelo endereço IP do servidor do Insight Remote Support.

# Verificar coletas

Coletas não são executadas automaticamente depois da descoberta. A HP recomenda que você execute uma coleta manualmente após a descoberta completa para verificar a conectividade. Execute o cronograma de coleta manualmente na guia Serviços de coleta → Agendamentos de coleta. Para obter mais informações sobre como agendar coletas, consulte a Ajuda do Insight RS.

Observe também que os sistemas StoreAll Storage usam coletas de configurações básicas do servidor no lugar de coletas de configurações de armazenamento.

Verifique se essa coleta foi bem-sucedida na guia Serviços de coleta → Resultados da coleta básica do Insight RS Console.

1. Faça logon no Insight RS Console.
2. No menu principal, selecione **Serviços de coleta** e depois clique na guia **Resultados da coleta básica**.
3. Expanda a seção Coleta de configurações básicas do servidor.
4. Localize a entrada referente ao seu dispositivo e verifique a coluna Resultado. Se a coleta tiver sido bem-sucedida, um ícone de êxito será exibido (). Se ocorrer uma falha, um ícone de erro será exibido ().

# Capítulo 28: Configurar sistemas de backup StoreOnce (D2D)

## Atender aos requisitos de configuração

Para configurar seus sistemas de backup StoreOnce (D2D) de forma que eles sejam monitorados pelo Insight RS, conclua as seguintes seções:

**Tabela 28.1** ***Etapas de configuração de sistemas de backup StoreOnce (D2D)***

| Tarefa | Concluída? |
|---|---|
| Certifique-se de que o Insight RS suporte seu sistema de backup StoreOnce (D2D), verificando o *Notas de Lançamento do HP Insight Remote Support*. | |
| Verifique a versão do firmware no sistema de backup StoreOnce (D2D). | |
| Configure o SNMP no sistema de backup StoreOnce (D2D). | |
| Adicione o protocolo SNMP ao Insight RS Console. | |
| Detecte o sistema StoreOnce Backup (D2D) no Insight RS Console. | |

## Instalar e configurar o software de comunicação em sistemas de backup

Para configurar seus dispositivos monitorados, conclua as seguintes seções:

## Verificar a versão do firmware

O Insight RS apenas oferece suporte a sistemas StoreOnce Backup que usam a versão de firmware 2.1.03 ou superior. Confira a versão do firmware na interface de usuário StoreOnce Backup, como mostrado abaixo. Se sua versão de firmware é anterior à versão 2.1.03, atualize seu firmware para uma versão suportada.

# Configurar o SNMP em sistemas de backup StoreOnce (D2D)

Você deve adicionar o dispositivo host como um destino de interceptação nos dois sistemas de backup D2D para que os eventos de serviço cheguem ao Insight RS.

## *Configurar o SNMP para sistemas de backup StoreOnce Gen2 (D2D)*

Para configurar o SNMP para sistemas de backup StoreOnce (D2D), siga estas etapas:

1. Faça logon no sistema de backup StoreOnce como "administrador" usando `https://`*<StoreOnce_ Backup_IP>*.
2. Clique na guia **Configuração**.
3. No painel **Configuração do dispositivo**, clique na guia **SNMP**.
4. Clique em **Editar** e habilite o agente SNMP, marcando a caixa de seleção **SNMP habilitado**.

5. Use o endereço IP do dispositivo host para adicionar um destino.

### Configurar o SNMP para sistemas de backup StoreOnce Gen3 B6200 e 2600/4200/4400

Para configurar os sistemas de backup StoreOnce B6200 e 2600/4200/4400 para enviar interceptações para o Insight Remote Support, conclua as seguintes etapas:

1. Faça logon no sistema de backup StoreOnce usando o protocolo SSH (usando "`putty.exe`" ou uma ferramenta semelhante).
2. Verifique a configuração atual do SNMP, emitindo o comando CLI: **`snmp show config`**.
3. Se o "State" (Estado) do SNMP for exibido como “off” (desligado), execute o comando CLI: **`snmp enable`**.
4. Para adicionar seu dispositivo host como um Destino de interceptação, use: **`snmp add trapsink`** ***<endereço IP do dispositivo host>*** **`events alert`**.
5. Verifique se a configuração atual do SNMP exibe o destino de interceptação que acaba de ser configurado usando: **`snmp show config`**.
6. Digite **`exit`** (sair) para encerrar a sessão.

# Adicionar credenciais de protocolo e iniciar a detecção

Para detectar seus dispositivos monitorados, conclua as seguintes seções:

## Criar uma credencial de protocolo SNMPv1 no Insight RS Console

Se a cadeia da comunidade SNMPv1 do dispositivo estiver definida como `pública` e o modo de acesso da comunidade for `somente leitura`, o Insight RS associará automaticamente um protocolo SNMP ao seu dispositivo. Se você usar uma cadeia de comunidade diferente ou uma porta não padrão, precisará criar uma credencial de protocolo SNMPv1 no Insight RS Console.

Para configurar o SNMPv1 no Insight RS Console, conclua as seguintes etapas:

1. Em um navegador da Web, faça logon no Insight RS Console.
2. No menu principal, selecione **Detecção** e clique na guia **Credenciais**.
3. Na lista suspensa Selecionar e configurar protocolo, selecione **Simple Network Management Protocol versão 1 (SNMPv1)**.
4. Clique em **Novo**. A caixa de diálogo Nova credencial é exibida.
5. Digite a cadeia de caracteres da comunidade configurada no seu dispositivo.
6. Clique em **Adicionar**.

O Insight RS cria a credencial de protocolo, que é exibida na tabela de credenciais.

# Detectar o dispositivo no Insight RS Console

Para detectar o dispositivo por meio do Insight RS Console, conclua as seguintes etapas:

1. Em um navegador da Web, faça logon no Insight RS Console.
2. No menu principal, selecione **Detecção** e clique na guia **Fontes**.
3. Expanda a seção Endereços IP e adicione o endereço IP do seu dispositivo:
   a. Clique em **Novo**.
   b. Selecione **Endereço único**, **Intervalo de endereços** ou **Lista de endereços**.
   c. Digite os endereços IP dos dispositivos a serem detectados.
   d. Clique em **Adicionar**.
4. Clique em **Iniciar detecção**.

# Verificar o status de detecção e do dispositivo

Para verificar se o dispositivo foi detectado corretamente, conclua as seguintes etapas:

1. Em um navegador da Web, faça logon no Insight RS Console.
2. No menu principal, selecione **Dispositivos** e clique na guia **Resumo do dispositivo**.
3. Verifique se a coluna Status contém um ícone de êxito ( ).

   Se não houver ícone de êxito, tente descobrir que coluna está com problema e consulte a Ajuda on-line para informações de solução de problemas.

# Capítulo 29: Configurar sistemas de biblioteca virtual

## Atender aos requisitos de configuração

Para configurar sistemas de biblioteca virtual de forma que eles sejam monitorados pelo Insight RS, conclua as seguintes seções:

**Tabela 29.1** ***Etapas de configuração do sistema de biblioteca virtual***

| Tarefa | Concluída? |
| --- | --- |
| Certifique-se de que o Insight RS suporte seu sistema de biblioteca virtual, verificando o *Notas de Lançamento do HP Insight Remote Support*. | |
| Configure o SNMP no sistema de biblioteca virtual. | |
| Detecte o sistema de biblioteca virtual no Insight RS Console. | |
| Envie um evento de teste para verificar a conectividade entre seu sistema de biblioteca virtual e o Insight RS. | |

# Instalar e configurar o software de comunicação em sistemas de biblioteca virtual

Para configurar seus dispositivos monitorados, conclua a seguinte seção:

## Configurar o SNMP no sistema de biblioteca virtual

Para suportar suas bibliotecas de fitas do Sistema de biblioteca virtual (VLS), é necessário configurar o SNMP no Command View Sistemas de biblioteca virtual (VLS).

Para configurar o SNMP nas suas bibliotecas de fitas VLS, siga estas instruções:

1. Faça logon na interface web do Command View VLS de cada nó VLS.
2. Clique na guia **Notificações**.
3. Clique na tarefa **Editar configurações SNMP**. Observe que essa tarefa pode ser chamada de **Configuração SNMP**, dependendo da sua versão do Command View VLS.

4. No campo **Nome do host**, digite o endereço IP ou FQDN do dispositivo host.
5. No campo **Cadeia de caracteres de comunidade**, se for selecionado um nome de comunidade de interceptação não-padrão (por exemplo, algo diferente de `public`), verifique se o Insight RS Console reconhece este nome.
6. A versão da interceptação é `1`.
7. Clique em **Adicionar**.

# Adicionar credenciais de protocolo e iniciar a detecção

Para detectar seus dispositivos monitorados, conclua as seguintes seções:

## Criar uma credencial de protocolo SNMPv1 no Insight RS Console

Se a cadeia da comunidade SNMPv1 do dispositivo estiver definida como `pública` e o modo de acesso da comunidade for `somente leitura`, o Insight RS associará automaticamente um protocolo SNMP ao seu dispositivo. Se você usar uma cadeia de comunidade diferente ou uma porta não padrão, precisará criar uma credencial de protocolo SNMPv1 no Insight RS Console.

Para configurar o SNMPv1 no Insight RS Console, conclua as seguintes etapas:

1. Em um navegador da Web, faça logon no Insight RS Console.
2. No menu principal, selecione **Detecção** e clique na guia **Credenciais**.
3. Na lista suspensa Selecionar e configurar protocolo, selecione **Simple Network Management Protocol versão 1 (SNMPv1)**.
4. Clique em **Novo**. A caixa de diálogo Nova credencial é exibida.
5. Digite a cadeia de caracteres da comunidade configurada no seu dispositivo.
6. Clique em **Adicionar**.

O Insight RS cria a credencial de protocolo, que é exibida na tabela de credenciais.

## Detectar o dispositivo no Insight RS Console

Para detectar o dispositivo por meio do Insight RS Console, conclua as seguintes etapas:

1. Em um navegador da Web, faça logon no Insight RS Console.
2. No menu principal, selecione **Detecção** e clique na guia **Fontes**.
3. Expanda a seção Endereços IP e adicione o endereço IP do seu dispositivo:
   a. Clique em **Novo**.
   b. Selecione **Endereço único**, **Intervalo de endereços** ou **Lista de endereços**.

c. Digite os endereços IP dos dispositivos a serem detectados.

d. Clique em **Adicionar**.

4. Clique em **Iniciar detecção**.

# Verificar o status de detecção e do dispositivo

Para verificar se o dispositivo foi detectado corretamente, conclua as seguintes etapas:

1. Em um navegador da Web, faça logon no Insight RS Console.
2. No menu principal, selecione **Dispositivos** e clique na guia **Resumo do dispositivo**.
3. Verifique se a coluna Status contém um ícone de êxito ( ).

   Se não houver ícone de êxito, tente descobrir que coluna está com problema e consulte a Ajuda on-line para informações de solução de problemas.

# Verificar a comunicação entre o dispositivo monitorado e o Insight RS

Para verificar a comunicação entre o dispositivo monitorado e o Insight RS, conclua as seguintes seções:

# Enviar um evento de teste para verificar a configuração

**Observação:** Não puxe uma FRU redundante para testar a configuração.

Se o firmware de VLS mais recente VLS e a última versão do Command View VLS estiverem instalados, clique no botão **Testar SNMP** na página de configuração do Command View VLS SNMP para realizar um teste de ponta a ponta. Esse evento de teste não resultará na criação de um caso na HP, mas criará uma notificação por e-mail local para confirmar que o VLS SNMP e o Insight Remote Support estão configurados corretamente.

# Verificar coletas no Insight RS Console

Coletas de configuração não têm suporte para esse tipo de dispositivo, exceto quando ele faz parte de uma coleta de SAN. Se você adicionou esse dispositivo a uma coleta de SAN, poderá executar manualmente uma coleta de SAN para verificar a configuração.

1. Faça logon no Insight RS Console.
2. No menu principal, selecione **Serviços de coleta**.
3. Clique na guia **Agendamentos de coleta**.
4. No painel Lista de agendamentos de coleta, selecione **Agendamento de coletas de configuração da SAN**. Informações sobre a coleta são exibidas no painel Informações da coleta. O painel Nestes dispositivos lista os dispositivos em que a coleta será executada.

5. No painel Informações de agendamento, clique em **Executar agora**.
6. Quando a coleta terminar, clique na guia **Resultados da Coleta de Armazenamento SAN**.
7. Expanda a seção Coleta de Configurações de SAN.
8. Localize a entrada referente ao seu dispositivo e verifique a coluna Resultado. Se a coleta tiver sido bem-sucedida, um ícone de êxito será exibido ( ). Se ocorrer uma falha, um ícone de erro será exibido ( ).

# Capítulo 30: Configurar bibliotecas de fita StoreEver

As bibliotecas de fitas físicas HP requerem uma combinação de suas próprias interfaces de gerenciamento baseadas na web e o software de gerenciamento de biblioteca HP Command View for Tape Libraries (TL) agregado, para funcionar com o Insight Remote Support (RS). Os usuários configuram cada biblioteca para enviar interceptações de SNMP para eventos de hardware, como falhas de ventoinha, diretamente para o servidor do Insight RS. Os usuários configuram o Command View TL para enviar eventos do TapeAssure pelo SMI-S, como pouca margem da unidade. Você precisa detectar o Command View TL e as bibliotecas separadamente.

**Observação:** O Insight RS não suporta unidades de fita independentes (fora da biblioteca).

## Atender aos requisitos de configuração

Para configurar o Command View TL TapeAssure e bibliotecas de fita de forma que eles sejam monitorados pelo Insight RS, conclua as seguintes seções:

**Observação:** Nas versões futuras, estas instruções serão simplificadas.

**Tabela 30.1** ***Etapas de configuração da bibliotecas de fitas***

| Tarefa | Concluída? |
|---|---|
| Certifique-se de que o Insight RS suporte sua biblioteca de fitas, verificando o *Notas de Lançamento do HP Insight Remote Support*. | |
| Configure o Command View TL TapeAssure. Observe que o Command View TL fornece o protocolo WBEM para suporte a coletas de configuração. | |
| Configure interceptações SNMPv1 em cada biblioteca de fita com o dispositivo host como destino da interceptação. | |
| Adicione o protocolo SNMP ao Insight RS Console. | |
| Adicione o protocolo WBEM ao Insight RS Console (para ESL e EML). | |
| Detecte a biblioteca de fitas no Insight RS Console. | |
| Verifique as informações de garantia e contrato no Insight RS Console. | |

## Instalar e configurar o software de comunicação em bibliotecas de fita

Para configurar seus dispositivos monitorados, conclua as seguintes seções:

### Configurar o Command View TL TapeAssure

Além de gerenciar as bibliotecas de fitas, o Command View para bibliotecas de fita fornece o protocolo

WBEM que é necessário para o Insight RS reunir coletas sobre as suas bibliotecas de fitas. Durante a descoberta das bibliotecas de fitas ou do servidor Command View TL, um protocolo WBEM deve ser criado no Insight RS Console para a instância do Command View TL no servidor, e o servidor de gerenciamento deve estar *ativamente* gerenciando as bibliotecas de fita para que as coletas sejam reunidas.

**Observação:** A HP recomenda que você use a versão mais recente do Command View TL. Baixe a atualização em: http://www.hp.com/support/cvtl.

**Importante:** Selecione Instalação personalizada para garantir que o provedor Command View TL SMI-S seja instalado.

Use o procedimento a seguir para configurar o Command View TL para permitir que o Insight RS se registre para eventos do TapeAssure para o Command View TL.

## Configurar o Command View TL 3.1 e versões posteriores

O Command View TL 3.1 CIMOM tem a autenticação de usuário habilitada. Com a autenticação ativada, o administrador do Open Pegasus CIMOM tem que criar usuários SMI-S e fornece privilégios de acesso para cada usuário. Qualquer usuário existente ou recém-criado do Windows pode se tornar um `cimuser`.

Para adicionar usuários e namespaces à autenticação do Command View TL 3.1 CIMOM, siga estas instruções:

1. Abra uma janela de comando e altere o diretório para: `C:\Program Files (x86)\Hewlett-Packard\Command View TL\op-cimom\bin`.
2. Para criar um usuário `cimuser`, use o comando:

   **`cimuser –a –u <nome de usuário do Windows>`**

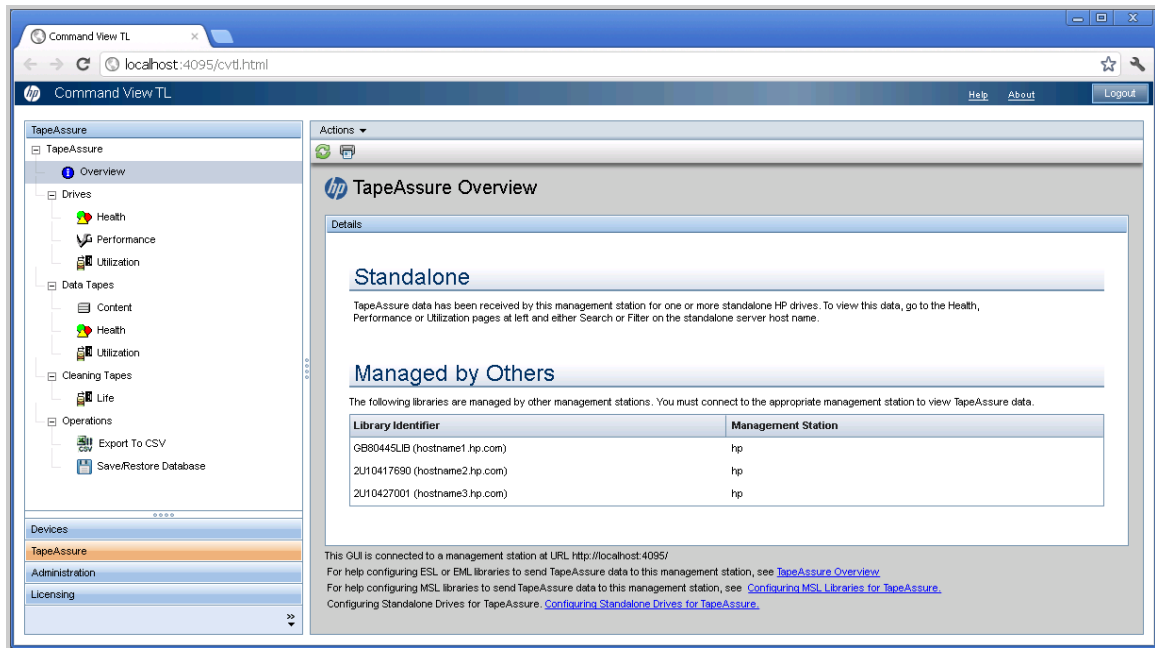
   O comando pede a senha e uma confirmação. Forneça a senha de sua escolha.
3. Forneça acesso de leitura/gravação aos namespaces. No TapeAssure Provider, todas as classes são implementadas em dois namespaces: `root/PG_Interop` e `root/hptl`. Ambos os namespaces devem receber acesso de leitura e escrita. Para permitir o acesso aos namespaces acima para um usuário selecionado, use o comando:

   **`cimauth –a -u <cimuser> -n <namespace> -R -W`**

## Verificar se o Command View TL está monitorando suas bibliotecas de fita

Para configurar o Command View TL TapeAssure de forma a monitorar cada biblioteca, siga estas instruções:

1. No Command View TL, adicione as bibliotecas de fitas a serem monitoradas na janela Command View TL Launcher. **Seleção de biblioteca** → **Ações** → **Adicionar biblioteca**.
2. Selecione a guia **TapeAssure** e verifique se as bibliotecas monitoradas são exibidas na janela Visão

geral do TapeAssure.

**Importante:** O TapeAssure também pode monitorar unidades de fita autônomas (que não estão em biblioteca de fitas), e um nome de host é exibido no lugar de um nome de biblioteca; no entanto, unidades autônomas não podem ser configuradas para o Insight RS.

# Configurar o SNMP nas bibliotecas de fitas

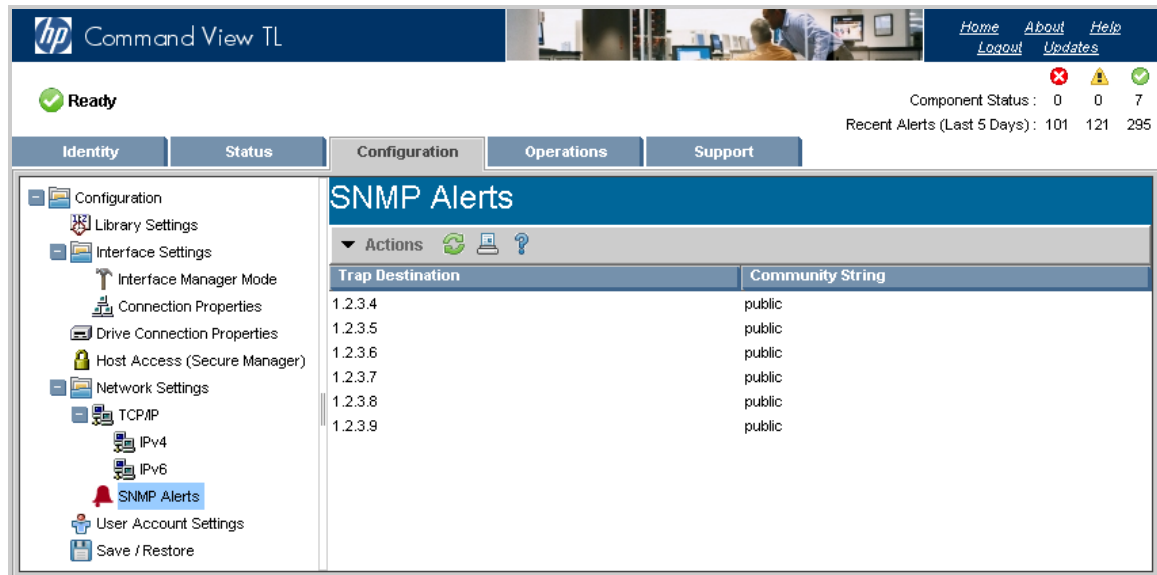
Você deve adicionar o dispositivo host como um destino de interceptação nas suas bibliotecas de fita para que os eventos de serviço cheguem ao Insight RS.

## *Configurar a Enterprise Systems Library série E e a Enterprise Modular Library*

Para permitir que o Insight RS se registre para eventos de integridade de biblioteca Enterprise Systems Library (ESL) série E ou na Enterprise Modular Library (EML) usando SNMP, o Command View TL deve estar configurado.

Para configurar o SNMP no Command View TL, siga estas instruções:

1. Faça logon na interface web do Command View TL para cada ESL-E ou EML.
2. Clique na guia **Configuração**.

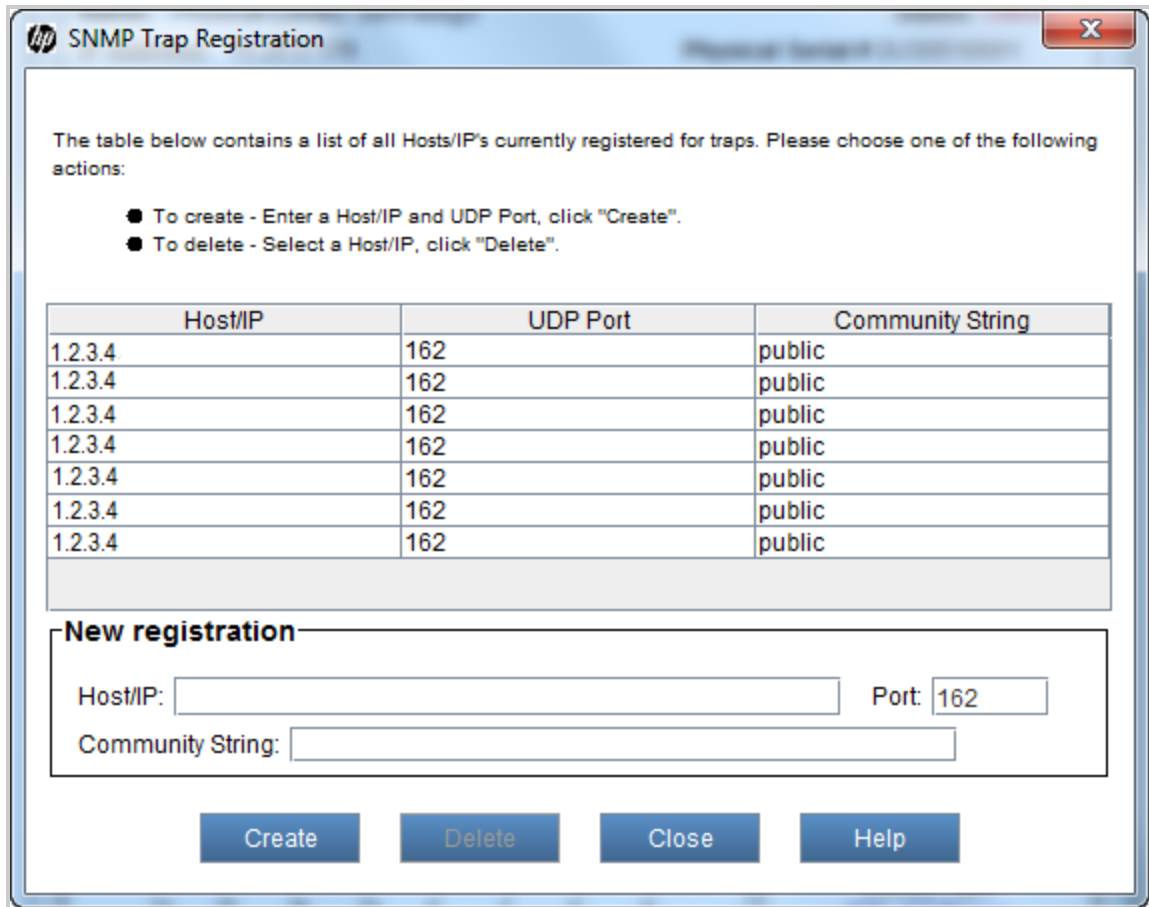
3. No painel esquerdo, selecione **Alertas SNMP**. As interceptações de SNMP atuais são exibidas no painel direito.

4. Siga um destes procedimentos:
   - No painel à direita, clique em uma interceptação de SNMP e selecione **Adicionar entrada de interceptação**.

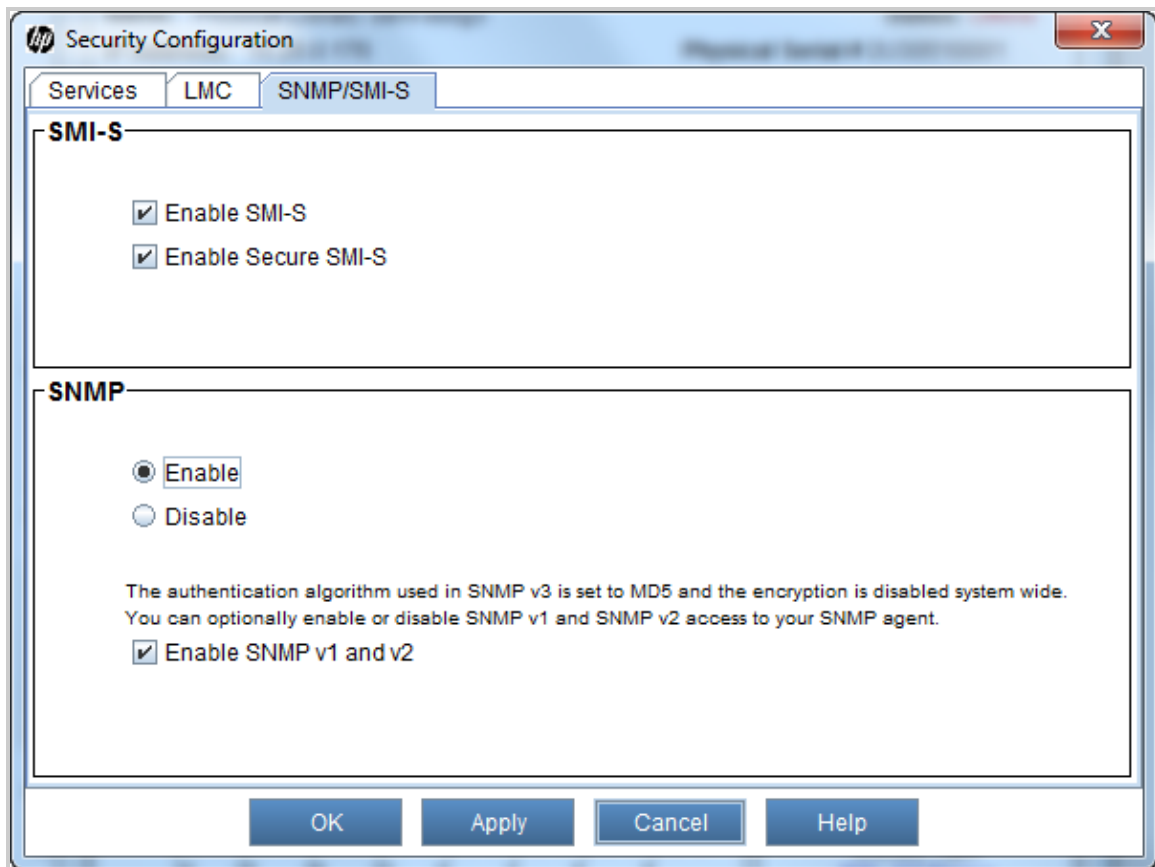
     *ou*
   - Selecione **Ações** → **Adicionar entrada de interceptação**.

   A tela **Entrada de interceptação de SNMP** é exibida.

5. No campo **Destino da interceptação**, digite o endereço IP ou o Nome de domínio totalmente qualificado (FQDN) do dispositivo host.
6. Digite `public` na **Cadeia da comunidade**, a menos que tenha sido definida outra cadeia de comunidade.
7. Clique em **OK**.

## Configurar a Enterprise Systems Library série G3

Para permitir que o Insight RS se registre para os eventos de integridade da biblioteca Enterprise Systems Library (ESL) G3 usando o SNMP, conclua as seguintes etapas:

1. Faça logon na interface do usuário do ESL G3 como `admin`.
2. No console, acesse **Configuração** → **Configuração de rede** → **Definições de segurança da rede**.
3. Na tela de Configuração de segurança, selecione a guia **SNMP/SMI-S**.

**Observação:** Os eventos de integridade da biblioteca são monitorados apenas com o SNMP. Você não precisa habilitar o SMI-S, a menos que ele seja necessário para outro software de gerenciamento de rede.

4. Clique em **OK**.
5. No console, acesse **Configuração** → **Notificações** → **Registro de interceptação de SNMP**.
6. Na tela Registro de interceptação de SNMP, crie uma interceptação de SNMPv1, na porta 162, de entrada para o endereço IP do dispositivo host. Use `public` para o nome da comunidade. Clique em **Criar**.

## Configurar a Modular Systems Library série G3

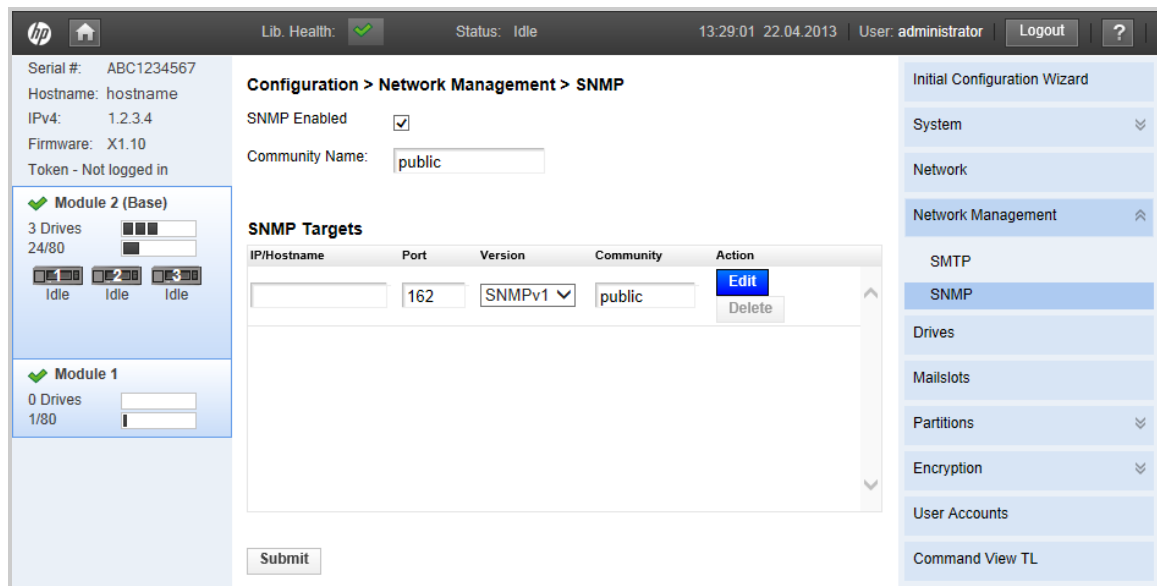
Para permitir que o Insight RS se registre para os eventos de integridade da biblioteca da Biblioteca de sistemas modulares (MSL) G3 usando SNMP, siga estas instruções:

1. Faça logon na interface web do Command View MSL como `Administrador`.
2. Clique na guia **Configuração**.
3. Clique na guia **Gerenciamento de rede**.

4. Verifique se a caixa de seleção **SNMP ativado** está marcada.
5. No campo de endereço **Destino IPv4**, digite o endereço IP ou FQDN do dispositivo host.
6. Verifique se **SNMPv1** é a versão selecionada.
7. Em **Filtro de notificação de interceptação de SNMP**, selecione **Eventos críticos e de aviso**, como o nível do filtro.
8. Clique em **Enviar**.

## Configurar a Biblioteca de sistemas modulares MSL6480

Para permitir que o Insight RS se registre para os eventos de integridade da biblioteca da Biblioteca de sistemas modulares (MSL) MSL6480 usando SNMP, siga estas instruções:

1. Faça login na interface da web do MSL6480 como `Administrador`.
2. Clique em **Configuração**.
3. Clique em **Gerenciamento de rede** → guia **SNMP**.

4. Verifique se a caixa de seleção **SNMP ativado** está marcada.
5. Na tabela **Destinos SNMP**, clique em **Editar**, próximo a um destino sem um IP/Nome de host.
6. No campo **IP/Nome de host**, digite o endereço IP ou FQDN do dispositivo host.
7. Verifique se **SNMPv1** é a versão selecionada e insira a cadeia de caracteres de comunidade do dispositivo host.
8. Clique em **Enviar**.
9. Clique em **OK**, na caixa de diálogo de confirmação.

# Definir configurações de firewall e porta

Para obter uma lista completa de requisitos de firewall e de porta para dispositivos monitorados, consulte o *Informe de Segurança do HP Insight Remote Support*, em: http://www.hp.com/go/insightremotesupport/docs.

# Adicionar credenciais de protocolo e iniciar a detecção

Para detectar seus dispositivos monitorados, conclua as seguintes seções:

## Criar uma credencial de protocolo SNMPv1 no Insight RS Console

Se a cadeia da comunidade SNMPv1 do dispositivo estiver definida como `pública` e o modo de acesso da comunidade for `somente leitura`, o Insight RS associará automaticamente um protocolo SNMP ao seu dispositivo. Se você usar uma cadeia de comunidade diferente ou uma porta não padrão, precisará criar uma credencial de protocolo SNMPv1 no Insight RS Console.

Para configurar o SNMPv1 no Insight RS Console, conclua as seguintes etapas:

1. Em um navegador da Web, faça logon no Insight RS Console.
2. No menu principal, selecione **Detecção** e clique na guia **Credenciais**.
3. Na lista suspensa Selecionar e configurar protocolo, selecione **Simple Network Management Protocol versão 1 (SNMPv1)**.
4. Clique em **Novo**. A caixa de diálogo Nova credencial é exibida.
5. Digite a cadeia de caracteres da comunidade configurada no seu dispositivo.
6. Clique em **Adicionar**.

O Insight RS cria a credencial de protocolo, que é exibida na tabela de credenciais.

# Criar uma credencial de protocolo WBEM no Insight RS Console

Para bibliotecas de fitas ESL e EML, você deve criar um protocolo WBEM no Insight RS Console para o servidor Command View TL que monitora suas bibliotecas de fitas.

Para configurar o WBEM no Insight RS Console, conclua as seguintes etapas:

1. Em um navegador da Web, faça logon no Insight RS Console.
2. No menu principal, selecione **Detecção** e clique na guia **Credenciais**.
3. Na lista suspensa **Selecionar e configurar protocolo**, selecione **Gerenciamento Corporativo baseado na Web (WBEM)**.
4. Clique em **Novo**. A caixa de diálogo Nova credencial é exibida.
5. Digite o nome de usuário e a senha configurados no seu dispositivo.
6. Clique em **Adicionar**.

O Insight RS cria a credencial de protocolo, que é exibida na tabela de credenciais.

# Detectar as bibliotecas de fita no Insight RS

O Insight RS não indica incidentes para as bibliotecas de fita ou o TapeAssure, a menos que eles sejam reconhecidos pelo Insight RS. Para garantir que o Insight RS indique incidentes, siga estas instruções:

1. Em um navegador da Web, faça logon no Insight RS Console.
2. No menu principal, selecione **Detecção** e clique na guia **Fontes**.
3. Digite os endereços IP a serem detectados:
   a. Digite o endereço IP do servidor host do Command View TL. Detecte o servidor host do Command View TL individualmente por seu endereço IP, garantindo que, quando você criar a tarefa de detecção do host do Command View TL, as credenciais de usuário do CIMOM criadas na seção "Configurar o Command View TL TapeAssure" sejam usadas.
   b. Digite os endereços IP das bibliotecas de fita. Detecte cada biblioteca individualmente ou dentro de um intervalo de endereços IP.
4. Clique em **Iniciar detecção**.

# Verificar informações de garantia e contrato

Após a detecção do dispositivo, verifique as informações de garantia e contrato.

1. Em um navegador da Web, faça logon no Insight RS Console.
2. No menu principal, selecione **Dispositivos** e clique na guia **Resumo do dispositivo**.
3. Verifique se todas as bibliotecas de fita monitoradas e os hosts do Command View TL aparecem na tabela de dispositivos.
4. Clique no nome do dispositivo e expanda o painel Hardware. Verifique se o número de produto e o número de série corretos da biblioteca de fitas foram detectados. Edite os dispositivos individuais se parecer que alguma informação de garantia e contrato estiver faltando.

**Importante:** Após a detecção, o `CVTL@`*<dispositivo>* listado pelo Insight RS sempre exibirá um ícone de erro ( ) em Garantia e contrato e na coluna de status.

# Verificar o status de detecção e do dispositivo

Para verificar se o dispositivo foi detectado corretamente, conclua as seguintes etapas:

1. Em um navegador da Web, faça logon no Insight RS Console.
2. No menu principal, selecione **Dispositivos** e clique na guia **Resumo do dispositivo**.
3. Verifique se a coluna Status contém um ícone de êxito ( ).

   Se não houver ícone de êxito, tente descobrir que coluna está com problema e consulte a Ajuda on-line para informações de solução de problemas.

# Verificar a comunicação entre o dispositivo monitorado e o Insight RS

Para verificar a comunicação entre o dispositivo monitorado e o Insight RS, conclua a seguinte seção:

# Verificar coletas no Insight RS Console

Coletas não são executadas automaticamente depois da descoberta. A HP recomenda que você execute uma coleta manualmente após a descoberta completa para verificar a conectividade. Execute o cronograma de coleta manualmente na guia Serviços de coleta → Agendamentos de coleta. Para obter mais informações sobre o agendamento de coletas, consulte a Ajuda do Insight RS.

Verifique se essa coleta foi bem-sucedida na guia Serviços de coleta → Resultados da Coleta de Armazenamento SAN no Insight RS Console.

1. Faça logon no Insight RS Console.
2. No menu principal, selecione **Serviços de coleta** e depois clique na guia **Resultados da Coleta de Armazenamento SAN**.
3. Expanda a seção Coleta de configurações de armazenamento.
4. Localize a entrada referente ao seu dispositivo e verifique a coluna Resultado. Se a coleta tiver sido bem-sucedida, um ícone de êxito será exibido ( ). Se ocorrer uma falha, um ícone de erro será exibido ( ).

# Capítulo 31: Configurar comutadores StoreFabric série B

## Atender aos requisitos de configuração

Para configurar seus comutadores StoreFabric série B de forma que eles sejam monitorados pelo Insight RS, conclua as seguintes seções:

**Observação:** O suporte para interceptação de teste para comutadores SAN série B requer a instalação do firmware Fabric Operating System v6.3.0b ou superior. Para obter mais detalhes, consulte o *Aviso aos clientes sobre o HP Fabric OS 6.3.0b*, em: http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?lang=en&cc=us&objectID=c01924282.

**Tabela 31.1** ***Etapas de configuração do comutador StoreFabric série B***

| Tarefa | Concluída? |
|---|---|
| Verifique se o Insight RS oferece suporte ao seu comutador série B, consultando as *Notas de Lançamento do HP Insight Remote Support*. | |
| Configure o SNMP no comutador série B. | |
| Adicione o protocolo SNMP ao Insight RS Console. | |
| Detecte o comutador da série B no Insight RS Console. | |
| Verifique o status do comutador da série B no Insight RS Console. | |
| Envie um evento de teste para verificar a conectividade entre o comutador série B e o Insight RS. | |

## Instalar e configurar o software de comunicação em comutadores de SAN

Para configurar seus dispositivos monitorados, conclua as seguintes seções:

## Configurar o SNMP

Use o procedimento a seguir para configurar o SNMP em um comutador da série B para que ele possa ser monitorado com o Insight Remote Support.

1. Exiba a versão do firmware do comutador:

   ```
   > version
   Fabric OS: v6.1.0c
   ```

2. Exiba as configurações atuais ou padrão do SNMPv1:

   ```
   > snmpconfig --show snmpv1
   ```

```
SNMPv1 community and trap recipient configuration:
Community 1: public (rw) No trap recipient configured yet
Community 2: public (rw) No trap recipient configured yet
Community 3: public (rw) No trap recipient configured yet
Community 4: public (ro) No trap recipient configured yet
Community 5: common (ro) No trap recipient configured yet
Community 6: FibreChannel (ro) No trap recipient configured yet
```

3. Defina a cadeia de caracteres de comunidade do SNMPv1 e o destinatário da interceptação:

```
> snmpconfig --set snmpv1
SNMP community and trap recipient configuration:
Community (rw): [public] gcc-public ! Create new community
Trap Recipient's IP address : [0.0.0.0] 1.2.3.4
Trap recipient Severity level : (0..5) [0] 2
Trap recipient Port : (0..65535) [162] Community (rw): [public]
Trap Recipient's IP address : [0.0.0.0] Community (rw): [public]
Trap Recipient's IP address : [0.0.0.0] Community (ro): [public]
Trap Recipient's IP address : [0.0.0.0] Community (ro): [common]
Trap Recipient's IP address : [0.0.0.0] Community (ro): [FibreChannel]
Trap Recipient's IP address : [0.0.0.0] Committing configuration...done.
```

**Observação:** O nível de gravidade da interceptação é associado ao endereço IP de cada destinatário da interceptação. O nível de interceptação de eventos está de acordo com o nível de gravidade do evento. Quando ocorre um evento e seu nível de severidade é igual ou inferior ao valor definido, as interceptações de eventos SNMP (`swEventTrap`, `swFabricWatchTrap` e `connUnitEventTrap`) são enviadas para os destinatários da interceptação.

Por padrão, esse valor é definido como 0, o que significa que essas interceptações não são enviadas. Estes são os valores possíveis:

- 0 nenhum
- 1 crítico
- 2 erro
- 3 aviso
- 4 informativo
- 5 depuração

4. Exiba as novas configurações:

```
> snmpconfig --show snmpv1
```

```
SNMPv1 community and trap recipient configuration:

Community 1: gcc-public (rw) Trap recipient: 1.2.3.4 Trap port: 162 Trap recipient
Severity level: 2

Community 2: public (rw) No trap recipient configured yet

Community 3: public (rw) No trap recipient configured yet

Community 4: public (ro) No trap recipient configured yet

Community 5: common (ro) No trap recipient configured yet

Community 6: FibreChannel (ro) No trap recipient configured yet
```

5. Defina o controle de acesso SNMP:

   **> snmpconfig --set accesscontrol**

   ```
   SNMP access list configuration:

   Access host subnet area: [11.0.0.2] 1.2.3.4 ! set to the IP add of SIM Read/Write?
   (true, t, false, f): [true]

   Access host subnet area: [1.2.3.4] Read/Write? (true, t, false, f): [true] f

   Access host subnet area: [1.2.3.4] Read/Write? (true, t, false, f): [true] f

   Access host subnet area: [1.2.3.4] 0.0.0.0 ! remove this one Read/Write? (true, t,
   false, f): [true] f

   Access host subnet area: [1.2.3.4] Read/Write? (true, t, false, f): [true]

   Access host subnet area: [1.2.3.4] Read/Write? (true, t, false, f): [true]

   Committing configuration...done.
   ```

6. Remova o endereço IP restante da lista de controle de acesso SNMP, caso necessário:

   **> snmpconfig --set accesscontrol**

   ```
   SNMP access list configuration:

   Access host subnet area: [1.2.3.4] Read/Write? (true, t, false, f): [true]

   Access host subnet area: [1.2.3.4] 0.0.0.0 Read/Write? (true, t, false, f):
   [false] f

   Access host subnet area: [1.2.3.4] 0.0.0.0 Read/Write? (true, t, false, f):
   [false] f

   Access host subnet area: [0.0.0.0] Read/Write? (true, t, false, f): [false]

   Access host subnet area: [1.2.3.4] 0.0.0.0 Read/Write? (true, t, false, f): [true]
   f

   Access host subnet area: [1.2.3.4] 0.0.0.0 Read/Write? (true, t, false, f): [true]
   f

   Committing configuration...done.
   ```

7. Verifique o acesso à lista de controle SNMP:

   **> snmpconfig --show accesscontrol**

   ```
   SNMP access list configuration:
   ```

```
Entry 0: Access host subnet area 1.2.3.4 (rw)
Entry 1: No access host configured yet
Entry 2: No access host configured yet
Entry 3: No access host configured yet
Entry 4: No access host configured yet
Entry 5: No access host configured yet
```

8. Defina o recurso MIB:

   ```
   > snmpconfig --set mibcapability
   The SNMP Mib/Trap Capability has been set to support FE-MIB SW-MIB FA-MIB HA-MIB
   SW-TRAP FA-TRAP HA-TRAP
   FA-MIB (yes, y, no, n): [yes]
   FICON-MIB (yes, y, no, n): [no]
   HA-MIB (yes, y, no, n): [yes] yes
   FCIP-MIB (yes, y, no, n): [no]
   ISCSI-MIB (yes, y, no, n): [no]
   SW-TRAP (yes, y, no, n): [yes]
   swFCPortScn (yes, y, no, n): [no] yes
   swEventTrap (yes, y, no, n): [no] yes
   swFabricWatchTrap (yes, y, no, n): [no] yes
   swTrackChangesTrap (yes, y, no, n): [no] yes
   FA-TRAP (yes, y, no, n): [yes]
   connUnitStatusChange (yes, y, no, n): [no] yes
   connUnitEventTrap (yes, y, no, n): [no] yes
   connUnitSensorStatusChange (yes, y, no, n): [no] yes
   connUnitPortStatusChange (yes, y, no, n): [no] yes
   SW-EXTTRAP (yes, y, no, n): [no] yes
   ```

9. Exiba o endereço IP do comutador, para que ele possa ser adicionado ao Insight RS Console:

   ```
   > ipaddrshow
   SWITCH Ethernet IP Address: 1.2.3.4
   Ethernet Subnetmask: 1.2.3.4
   Fibre Channel IP Address: none
   Fibre Channel Subnetmask: none
   Gateway IP Address: 1.2.3.4
   DHCP: Off
   ```

10. Modifique as variáveis `systemgroup` do comutador, caso necessário:

```
> snmpconfig --set systemGroup
Customizing MIB-II system variables ... At each prompt, do one of the following:
o to accept current value,
o enter the appropriate new value,
o to skip the rest of configuration, or
o to cancel any change.
To correct any input mistake: erases the previous character, erases the whole
line,
sysDescr: [Fibre Channel Switch.] Brocade 4/16 FC Switch
sysLocation: [End User Premise.] HP Building 11th floor
sysContact: [Field Support.] John Doe
authTrapsEnabled (true, t, false, f): [true]
Committing configuration...done.
```

# Definir configurações de firewall e porta

Para obter uma lista completa de requisitos de firewall e de porta para dispositivos monitorados, consulte o *Informe de Segurança do HP Insight Remote Support*, em: http://www.hp.com/go/insightremotesupport/docs.

# Adicionar credenciais de protocolo e iniciar a detecção

Para detectar seus dispositivos monitorados, conclua as seguintes seções:

# Criar uma credencial de protocolo SNMPv1 no Insight RS Console

Se a cadeia da comunidade SNMPv1 do dispositivo estiver definida como `pública` e o modo de acesso da comunidade for `somente leitura`, o Insight RS associará automaticamente um protocolo SNMP ao seu dispositivo. Se você usar uma cadeia de comunidade diferente ou uma porta não padrão, precisará criar uma credencial de protocolo SNMPv1 no Insight RS Console.

Para configurar o SNMPv1 no Insight RS Console, conclua as seguintes etapas:

1. Em um navegador da Web, faça logon no Insight RS Console.
2. No menu principal, selecione **Detecção** e clique na guia **Credenciais**.
3. Na lista suspensa Selecionar e configurar protocolo, selecione **Simple Network Management Protocol versão 1 (SNMPv1)**.
4. Clique em **Novo**. A caixa de diálogo Nova credencial é exibida.

5. Digite a cadeia de caracteres da comunidade configurada no seu dispositivo.
6. Clique em **Adicionar**.

O Insight RS cria a credencial de protocolo, que é exibida na tabela de credenciais.

# Detectar o dispositivo no Insight RS Console

Para detectar o dispositivo por meio do Insight RS Console, conclua as seguintes etapas:

1. Em um navegador da Web, faça logon no Insight RS Console.
2. No menu principal, selecione **Detecção** e clique na guia **Fontes**.
3. Expanda a seção Endereços IP e adicione o endereço IP do seu dispositivo:
   a. Clique em **Novo**.
   b. Selecione **Endereço único**, **Intervalo de endereços** ou **Lista de endereços**.
   c. Digite os endereços IP dos dispositivos a serem detectados.
   d. Clique em **Adicionar**.
4. Clique em **Iniciar detecção**.

# Verificar o status de detecção e do dispositivo

Para verificar se o dispositivo foi detectado corretamente, conclua as seguintes etapas:

1. Em um navegador da Web, faça logon no Insight RS Console.
2. No menu principal, selecione **Dispositivos** e clique na guia **Resumo do dispositivo**.
3. Verifique se a coluna Status contém um ícone de êxito ( ).

   Se não houver ícone de êxito, tente descobrir que coluna está com problema e consulte a Ajuda on-line para informações de solução de problemas.

# Verificar informações de garantia e contrato

Verifique se as informações de garantia e contrato foram detectadas corretamente no Insight RS Console:

1. No Insight RS Console, navegue até **Dispositivos** e clique na opção Nome do dispositivo.
2. Expanda a seção Hardware e confira se o **Número de série adquirido** e o **Número do produto adquirido** estão corretos. Se eles não estiverem corretos, digite os valores corretos nos campos **Substituir número de série** e **Substituir número do produto** e clique em **Salvar alterações**.

# Verificar a comunicação entre o dispositivo monitorado e o Insight RS

Para verificar a comunicação entre o dispositivo monitorado e o Insight RS, conclua as seguintes seções:

## Enviar um evento de teste

Desde o lançamento do Fabric-OS série B v6.3.x, os comutadores da série B podem emitir testes de interceptação para garantir que todo o fluxo de eventos de ponta a ponta possa ser verificado. O usuário deve fazer logon na interface de administrador de CLI do comutador e emitir este comando:

Envie interceptações de SNMP para testar a configuração:

1. Telnet ou SSH com o comutador da série B.
2. Mostre as interceptações disponíveis que você pode enviar como testes:

   **`snmptraps --show`**
3. Envie uma interceptação de teste geral para todos os testes:

   **`snmptraps --send`**
4. Ou envie uma interceptação de teste específica:

   **snmptraps --send --trap_name <*nomedainterceptação*>**

   Por exemplo:

   **snmptraps --send -trap_name cp-status-change-trap -ip_address <*ip_do_dispositivo_host*>**

   em que <*ip_do_dispositivo_host*> é o endereço IP do dispositivo host. Se o comutador relatar que não foi possível enviar a interceptação de teste, verifique se `snmpmibcaps` está configurado para o envio de interceptações HA. Se a configuração estiver correta, o comando deverá criar um evento de teste visível no Insight RS Console e enviar um incidente à HP.

---

**Observação:** Nem todas as interceptações resultam na entrega de um incidente ao Insight RS Console. Nem todas as interceptações são enviadas, e nem todas são recebidas. Algumas são recebidas como 'evento não registrado', caso você tenha selecionado essa opção como opção de recebimento em Eventos. Os eventos exibidos como 'não registrados' não são compilados nos SIM Mibs. Os FA-MIBs geram um evento de hardware válido.

---

Consulte a documentação do comutador série B, para mais detalhes.

## Verificar coletas no Insight RS Console

Coletas não são executadas automaticamente depois da descoberta. A HP recomenda que você execute uma coleta manualmente após a descoberta completa para verificar a conectividade. Execute o cronograma de coleta manualmente na guia Serviços de coleta → Agendamentos de coleta. Para obter mais informações sobre o agendamento de coletas, consulte a Ajuda do Insight RS.

Verifique se essa coleta foi bem-sucedida na guia Serviços de coleta → Resultados da Coleta de Armazenamento SAN no Insight RS Console.

1. Faça logon no Insight RS Console.
2. No menu principal, selecione **Serviços de coleta** e depois clique na guia **Resultados da Coleta de Armazenamento SAN**.
3. Expanda a seção Coleta de configurações de armazenamento.
4. Localize a entrada referente ao seu dispositivo e verifique a coluna Resultado. Se a coleta tiver sido bem-sucedida, um ícone de êxito será exibido ( ). Se ocorrer uma falha, um ícone de erro será exibido ( ).

# Capítulo 32: Configurar comutadores StoreFabric série C

## Atender aos requisitos de configuração

Para configurar seus comutadores StoreFabric série C de forma que eles sejam monitorados pelo Insight RS, conclua as seguintes seções:

**Tabela 32.1** ***Etapas de configuração do comutador StoreFabric série C***

| Tarefa | Concluída? |
|---|---|
| Verifique se o Insight RS oferece suporte ao seu comutador série C, consultando as *Notas de Lançamento do HP Insight Remote Support*. | |
| Configure o SNMP no comutador série C. | |
| Adicione o protocolo SNMP ao Insight RS Console. | |
| Detecte o comutador da série C no Insight RS Console. | |
| Verifique o status do comutador da série C no Insight RS Console. | |
| Envie um evento de teste para verificar a conectividade entre o comutador série C e o Insight RS. | |

## Instalar e configurar o software de comunicação em comutadores de SAN

Para configurar seus dispositivos monitorados, conclua as seguintes seções:

## Configurar o SNMP

Para configurar o SNMP série C (o antigo Cisco), conclua as seguintes etapas:

1. Registre-se na interface de CLI com Telnet ou use o Fabric Manager.
2. Use os comandos de CLI `config t` e `snmp-server host <IP> traps version 1 public udp-port 162` para adicionar o endereço IP do dispositivo host como um destino de interceptação.
3. Escolha que todos os eventos retornem como interceptações.
4. Se você escolher um nome de comunidade de interceptação não padrão (por exemplo, um nome diferente de `public`), verifique se esse nome é usado nas configurações de credenciais do Insight RS Console.
5. Digite o endereço de IP do dispositivo host em umas das configurações de destino de interceptação. Essa configuração também pode ser feita com o Gerenciador de Dispositivos da Série C.
6. Detecte o dispositivo no Insight RS Console.
7. No Insight RS Console, navegue até **Dispositivos** e clique no nome do dispositivo. Verifique se as informações do dispositivo foram detectadas corretamente.

# Definir configurações de firewall e porta

Para obter uma lista completa de requisitos de firewall e de porta para dispositivos monitorados, consulte o *Informe de Segurança do HP Insight Remote Support*, em: http://www.hp.com/go/insightremotesupport/docs.

# Adicionar credenciais de protocolo e iniciar a detecção

Para detectar seus dispositivos monitorados, conclua as seguintes seções:

# Criar uma credencial de protocolo SNMPv1 no Insight RS Console

Se a cadeia da comunidade SNMPv1 do dispositivo estiver definida como `pública` e o modo de acesso da comunidade for `somente leitura`, o Insight RS associará automaticamente um protocolo SNMP ao seu dispositivo. Se você usar uma cadeia de comunidade diferente ou uma porta não padrão, precisará criar uma credencial de protocolo SNMPv1 no Insight RS Console.

Para configurar o SNMPv1 no Insight RS Console, conclua as seguintes etapas:

1. Em um navegador da Web, faça logon no Insight RS Console.
2. No menu principal, selecione **Detecção** e clique na guia **Credenciais**.
3. Na lista suspensa Selecionar e configurar protocolo, selecione **Simple Network Management Protocol versão 1 (SNMPv1)**.
4. Clique em **Novo**. A caixa de diálogo Nova credencial é exibida.
5. Digite a cadeia de caracteres da comunidade configurada no seu dispositivo.
6. Clique em **Adicionar**.

O Insight RS cria a credencial de protocolo, que é exibida na tabela de credenciais.

# Detectar o dispositivo no Insight RS Console

Para detectar o dispositivo por meio do Insight RS Console, conclua as seguintes etapas:

1. Em um navegador da Web, faça logon no Insight RS Console.
2. No menu principal, selecione **Detecção** e clique na guia **Fontes**.
3. Expanda a seção Endereços IP e adicione o endereço IP do seu dispositivo:
   a. Clique em **Novo**.
   b. Selecione **Endereço único**, **Intervalo de endereços** ou **Lista de endereços**.
   c. Digite os endereços IP dos dispositivos a serem detectados.
   d. Clique em **Adicionar**.
4. Clique em **Iniciar detecção**.

# Verificar o status de detecção e do dispositivo

Para verificar se o dispositivo foi detectado corretamente, conclua as seguintes etapas:

1. Em um navegador da Web, faça logon no Insight RS Console.
2. No menu principal, selecione **Dispositivos** e clique na guia **Resumo do dispositivo**.
3. Verifique se a coluna Status contém um ícone de êxito (✅).

   Se não houver ícone de êxito, tente descobrir que coluna está com problema e consulte a Ajuda on-line para informações de solução de problemas.

# Verificar informações de garantia e contrato

Verifique se as informações de garantia e contrato foram detectadas corretamente no Insight RS Console:

1. No Insight RS Console, navegue até **Dispositivos** e clique na opção Nome do dispositivo.
2. Expanda a seção Hardware e confira se o **Número de série adquirido** e o **Número do produto adquirido** estão corretos. Se eles não estiverem corretos, digite os valores corretos nos campos **Substituir número de série** e **Substituir número do produto** e clique em **Salvar alterações**.

# Verificar a comunicação entre o dispositivo monitorado e o Insight RS

Para verificar a comunicação entre o dispositivo monitorado e o Insight RS, conclua as seguintes seções:

# Enviar um evento de teste

**Observação:** Não puxe uma FRU redundante para testar a configuração.

Recentemente, a Cisco apresentou um comando de teste CLI para validar a conectividade do evento de uma ponta a outra do dispositivo.

1. No prompt CLI, emita o seguinte comando:

   ```
   test pfm test-SNMP-trap power
   ```

2. Isso fará com que o comutador da série C envie um evento de teste de `fonte de alimentação defeituosa` para o dispositivo host. Se tudo estiver configurado corretamente, esse evento resultará em um incidente visível para a HP.

**Observação:** você também pode usar **test pfm test-SNMP-trap fan**, mas o evento do tipo `temp`, se usado, será ignorado.

**Observação:** A primeira interceptação de teste Cisco será encaminhada pelo Insight Remote Support para a HP, mas testes de interceptação subsequentes serão omitidos por 24 horas até que outra interceptação de teste possa ser encaminhada para a HP.

# Verificar coletas no Insight RS Console

Coletas não são executadas automaticamente depois da descoberta. A HP recomenda que você execute uma coleta manualmente após a descoberta completa para verificar a conectividade. Execute o cronograma de coleta manualmente na guia Serviços de coleta → Agendamentos de coleta. Para obter mais informações sobre o agendamento de coletas, consulte a Ajuda do Insight RS.

Verifique se essa coleta foi bem-sucedida na guia Serviços de coleta → Resultados da Coleta de Armazenamento SAN no Insight RS Console.

1. Faça logon no Insight RS Console.
2. No menu principal, selecione **Serviços de coleta** e depois clique na guia **Resultados da Coleta de Armazenamento SAN**.
3. Expanda a seção Coleta de configurações de armazenamento.
4. Localize a entrada referente ao seu dispositivo e verifique a coluna Resultado. Se a coleta tiver sido bem-sucedida, um ícone de êxito será exibido ( ). Se ocorrer uma falha, um ícone de erro será exibido ( ).

# Capítulo 33: Configurar comutadores StoreFabric série H

## Atender aos requisitos de configuração

Para configurar os comutadores StoreFabric série H de forma que eles sejam monitorados pelo Insight RS, conclua as seguintes seções:

**Tabela 33.1** ***Etapas de configuração do comutador StoreFabric série H***

| Tarefa | Concluída? |
| --- | --- |
| Verifique se o Insight RS oferece suporte ao seu comutador série H, consultando as *Notas de Lançamento do HP Insight Remote Support*. | |
| Configure o SNMP no comutador série H. | |
| Adicione o protocolo SNMP ao Insight RS Console. | |
| Detecte o comutador da série H no Insight RS Console. | |
| Verifique o status do comutador da série H no Insight RS Console. | |

## Instalar e configurar o software de comunicação em comutadores de SAN

Para configurar seus dispositivos monitorados, conclua as seguintes seções:

## Configurar o SNMP

Faça login no comutador com Telnet e emita os seguintes comandos CLI para configurar os comutadores HP SN6000, 8/20q ou 2/8q FC de forma a enviar interceptações SNMP ao dispositivo host.

1. Abra a sessão do Admin:

   ```
   admin start
   ```

2. Configure os destinos de interceptações de SNMP:

   ```
   set setup snmp
   ```

3. Depois da configuração, digite **y** para salvar e ativar a configuração SNMP.
4. Feche a sessão do Admin:

   ```
   admin end
   ```

## Definir configurações de firewall e porta

Para obter uma lista completa de requisitos de firewall e de porta para dispositivos monitorados, consulte o *Informe de Segurança do HP Insight Remote Support*, em: http://www.hp.com/go/insightremotesupport/docs.

# Adicionar credenciais de protocolo e iniciar a detecção

Para detectar seus dispositivos monitorados, conclua as seguintes seções:

## Criar uma credencial de protocolo SNMPv1 no Insight RS Console

Se a cadeia da comunidade SNMPv1 do dispositivo estiver definida como `pública` e o modo de acesso da comunidade for `somente leitura`, o Insight RS associará automaticamente um protocolo SNMP ao seu dispositivo. Se você usar uma cadeia de comunidade diferente ou uma porta não padrão, precisará criar uma credencial de protocolo SNMPv1 no Insight RS Console.

Para configurar o SNMPv1 no Insight RS Console, conclua as seguintes etapas:

1. Em um navegador da Web, faça logon no Insight RS Console.
2. No menu principal, selecione **Detecção** e clique na guia **Credenciais**.
3. Na lista suspensa Selecionar e configurar protocolo, selecione **Simple Network Management Protocol versão 1 (SNMPv1)**.
4. Clique em **Novo**. A caixa de diálogo Nova credencial é exibida.
5. Digite a cadeia de caracteres da comunidade configurada no seu dispositivo.
6. Clique em **Adicionar**.

O Insight RS cria a credencial de protocolo, que é exibida na tabela de credenciais.

## Detectar o dispositivo no Insight RS Console

Para detectar o dispositivo por meio do Insight RS Console, conclua as seguintes etapas:

1. Em um navegador da Web, faça logon no Insight RS Console.
2. No menu principal, selecione **Detecção** e clique na guia **Fontes**.
3. Expanda a seção Endereços IP e adicione o endereço IP do seu dispositivo:
   a. Clique em **Novo**.
   b. Selecione **Endereço único**, **Intervalo de endereços** ou **Lista de endereços**.
   c. Digite os endereços IP dos dispositivos a serem detectados.
   d. Clique em **Adicionar**.
4. Clique em **Iniciar detecção**.

## Verificar o status de detecção e do dispositivo

Para verificar se o dispositivo foi detectado corretamente, conclua as seguintes etapas:

1. Em um navegador da Web, faça logon no Insight RS Console.
2. No menu principal, selecione **Dispositivos** e clique na guia **Resumo do dispositivo**.
3. Verifique se a coluna Status contém um ícone de êxito ().

   Se não houver ícone de êxito, tente descobrir que coluna está com problema e consulte a Ajuda on-line para informações de solução de problemas.

# Verificar informações de garantia e contrato

Verifique se as informações de garantia e contrato foram detectadas corretamente no Insight RS Console:

1. No Insight RS Console, navegue até **Dispositivos** e clique na opção Nome do dispositivo.
2. Expanda a seção Hardware e confira se o **Número de série adquirido** e o **Número do produto adquirido** estão corretos. Se eles não estiverem corretos, digite os valores corretos nos campos **Substituir número de série** e **Substituir número do produto** e clique em **Salvar alterações**.

# Verificar a comunicação entre o dispositivo monitorado e o Insight RS

Para verificar a comunicação entre o dispositivo monitorado e o Insight RS, conclua a seguinte seção:

## Verificar coletas no Insight RS Console

Coletas não são executadas automaticamente depois da descoberta. A HP recomenda que você execute uma coleta manualmente após a descoberta completa para verificar a conectividade. Execute o cronograma de coleta manualmente na guia Serviços de coleta → Agendamentos de coleta. Para obter mais informações sobre o agendamento de coletas, consulte a Ajuda do Insight RS.

Verifique se essa coleta foi bem-sucedida na guia Serviços de coleta → Resultados da Coleta de Armazenamento SAN no Insight RS Console.

1. Faça logon no Insight RS Console.
2. No menu principal, selecione **Serviços de coleta** e depois clique na guia **Resultados da Coleta de Armazenamento SAN**.
3. Expanda a seção Coleta de configurações de armazenamento.
4. Localize a entrada referente ao seu dispositivo e verifique a coluna Resultado. Se a coleta tiver sido bem-sucedida, um ícone de êxito será exibido (). Se ocorrer uma falha, um ícone de erro será exibido ().

# Capítulo 34: Configurar comutadores de rede baseados no ProVision

Comutadores de rede baseados no ProVision (anteriormente E-Series/ProCurve) exigem o SNMP para detecção e monitoramento de eventos. Os comutadores baseados no ProVision vêm de fábrica com o SNMP instalado e habilitado.

Você pode usar Telnet ou SSH para coletas de configurações. O Telnet vem habilitado por padrão nos comutadores baseados no ProVision. Se quiser usar o SSH para coletas de configurações, você terá que ativá-lo (consulte a seção "Habilitar o SSH").

## Atender aos requisitos de configuração

Para configurar seus comutadores de rede baseados no ProVisio de forma que eles sejam monitorados pelo Insight RS, conclua as seguintes seções:

**Tabela 34.1** ***Etapas de configuração de comutadores de rede baseados no ProVision***

| Tarefa | Concluída? |
|---|---|
| Certifique-se de que o Insight RS dê suporte ao seu comutador baseado no ProVision, verificando o *Notas de Lançamento do HP Insight Remote Support*. | |
| Crie senhas de Operador/Gerente no comutador. | |
| Configure o SSH no comutador. | |
| Configure o SNMP no comutador. | |
| Adicione os protocolos Telnet ou SSH e SNMP ao Insight RS Console. | |
| Detecte o comutador baseado no ProVision no Insight RS Console. | |

## Instalar e configurar o software de comunicação em comutadores

Para configurar seus dispositivos monitorados, conclua as seguintes seções:

## Criar senhas de operador/gerente

É obrigatório definir a senha de gerente.

Para definir uma senha de gerente, siga estas instruções:

1. Digite o comando **password all**. Você será solicitado a digitar as senhas de gerente e operador:

   ```
   # password all
   ```

2. Digite o comando **password manager** para definir a senha de gerente:

   ```
   # password manager
   ```

# Configurar o SSH

## Gerar a chave pública/privada do SSH

1. Digite o comando **config** para habilitar o modo de configuração global:

   ```
   # config
   ```

2. Digite o comando **crypto** para gerar um par de chaves RSA, que inclui uma chave RSA pública e uma chave RSA privada.

   ```
   # crypto key generate ssh rsa
   ```

## Habilitar o SSH

Você só precisa habilitar o SSH se quiser usá-lo no lugar do Telnet. Se preferir usar o Telnet, ignore esta seção.

Para habilitar o SSH, execute os seguintes comandos na linha de comando do comutador:

1. Digite o comando **config** para habilitar o modo de configuração global:

   ```
   # config
   ```

2. Habilite o servidor SSH:

   ```
   # ip ssh
   ```

3. Digite o comando write memory para salvar as alterações de configuração:

   ```
   # write mem
   ```

Para obter mais informações sobre comutadores baseados no ProVision, consulte a documentação do comutador baseado no ProVision, em: http://h17007.www1.hp.com/us/en/products/switches/index.aspx.

## Verificar a comunicação por Telnet/SSH

Para verificar se a comunicação por Telnet ou SSH está funcionando corretamente, conclua as seguintes etapas:

1. A partir do dispositivo host, conecte-se ao comutador baseado no ProVision usando o protocolo que você deseja verificar. Aguarde até que a conexão seja estabelecida.
2. Informe o `username` (nome de usuário) e a `password` (senha) quando solicitado. Se uma das mensagens a seguir for exibida, ela será considerada uma falha de login:
   - `Login incorrect (Login incorreto)`
   - `User authorization failure (Falha de autorização de usuário)`
   - `Invalid login name (nome de login inválido)`
   - `Too many users logged on already (Usuários demais já conectados)`
3. Quando os dados de login ou banner forem recebidos, envie um retorno de carro (\n) para ter certeza

de que o host está pronto.

4. Digite o comando `exit` para desconectar-se.

# Configurar comunicação por SNMP

Comutadores de rede baseados no ProVision podem ser configurados para usar SNMPv1, SNMPv2 ou SNMPv3. Selecione um dos métodos abaixo:

## *Configurar o SNMPv1/v2*

Para definir os dispositivos host como destino de interceptação e verificar se a comunicação SNMP está funcionando corretamente, conclua as seguintes etapas:

1. Digite o comando **show version** para determinar qual versão do software o seu comutador baseado no ProVision está executando:

   ```
   # sho ver
   ```

2. Digite o comando **config** para habilitar o modo de configuração global:

   ```
   # config
   ```

3. A saída deve mostrar um número de versão semelhante a *x*.14.60, onde *x* será uma letra como K.
4. Use o comando **snmp-server** para digitar o endereço IP do dispositivo host. Dependendo da versão do firmware no comutador baseado no ProVision, use uma das seguintes versões do comando:

| Versão do firmware | Comando |
| --- | --- |
| **14.60 ou inferior** | **# snmp-server host <*endereço IP*> public not-info** |
| **14.61 e superior** | **# snmp-server host <*endereço IP*> community public trap-level not-info** |

5. Verifique se as configurações que você digitou foram salvas:

   ```
   # sho run
   ```

6. Digite o comando write memory para salvar as alterações de configuração:

   ```
   # write mem
   ```

## *Configurar o SNMPv3*

Para definir os dispositivos host como destino de interceptação e verificar se a comunicação SNMP está funcionando corretamente, conclua as seguintes etapas:

1. Habilite o SNMPv3:

   ```
   # snmpv3 enable
   ```

2. Configure os usuários SNMP apropriados:

   ```
   # snmpv3 user <user-name> [auth <md5 | sha> <auth-pass>] [priv <priv-pass>]
   ```

3. Configure os grupos SNMP apropriados:

```
# snmpv3 group group <group-name> user <user-name> sec-model ver3
```

4. Configure os receptores de interceptação apropriados:

```
# snmpv3 notify <notify-name> tag <tag-name>
# snmpv3 targetaddress <name> params <parms-name> <ip-addr>
# snmpv3 params <params-name> user <user-name>
```

# Configurar a autenticação de chave pública do SSH

## *Opção 1: Usar o certificado do dispositivo host*

### *Pré-requisitos*

- *Servidor TFTP* — usado para mover a chave pública para o comutador baseado no ProVision.

### *Copiar o certificado para o comutador*

Para copiar o certificado para o comutador baseado no ProVision, siga estas etapas:

1. No dispositivo host, exporte a chave pública do dispositivo host. O nome de alias é "jetty":

   ```
   rsadmin cert -export -keycomment manager@[IP_do_comutador] -sshkey -out [nome_do_caminho_do_arquivo]
   ```

   em que *nome_do_caminho_do_arquivo* é um caminho que possa ser visto pelo servidor TFTP.
2. Conecte-se ao comutador via Telnet ou SSH usando a autenticação por nome de usuário/senha.
3. Entre no modo de configuração:

   ```
   configure
   ```
4. Desative a transferência de arquivos por SSH:

   ```
   no ip ssh filetransfer
   ```
5. Habilite o cliente TFTP:

   ```
   tftp client
   ```
6. Mova a chave pública para o comutador:

   ```
   copy tftp pub-key-file <ip_servidor_tftp> <arquivo_de_chave_pública> manager
   ```
7. Habilite a autenticação de chave pública:

   ```
   aaa authentication ssh login public-key
   ```
8. Habilite a autenticação por usuário/senha:

   ```
   aaa authentication ssh enable local
   ```
9. Grave a configuração e a chave pública na memória:

   ```
   wr mem
   ```

### *Criar uma credencial de protocolo SSH no Insight RS Console*

Para configurar o SSH no Insight RS Console, conclua as seguintes etapas:

1. No Insight RS Console, adicione uma credencial de certificado SSH na guia **Detecção → Credenciais**.

a. Na lista suspensa **Selecionar e configurar protocolo**, selecione **Secure Shell (SSH)** e clique em **Novo**.

b. Na lista suspensa **Tipo**, selecione **Credencial de certificado**.

c. Deixe o campo **Carregar arquivo** em branco, porque o certificado já está no repositório de certificados e é identificado usando-se o nome de alias.

d. Digite o alias de certificado “jetty-manager”, que foi o alias dado ao certificado quando ele foi exportado acima.

2. Clique em **Adicionar**.

# *Opção 2: Usar outros certificados*

## *Pré-requisitos*

- *PuTTYgen* — usado para gerar um par de chaves, caso necessário.
- *Servidor TFTP* — usado para mover a chave pública para o comutador baseado no ProVision.

## *Copiar o certificado para o comutador*

Para copiar o certificado para o comutador baseado no ProVision, siga estas etapas:

1. Use o PuTTYgen para criar um par de chaves.
2. Altere o campo de comentário de chave pública em PuTTYgen para `manager@IP` para o acesso da

conta do operador, em que IP é o IP do comutador, ou `manager@ip` para o acesso da conta do gerente.

3. Copie a chave pública para um caminho de arquivo que seu servidor TFTP possa ver. (Consulte a documentação do servidor TFTP e a configuração do servidor para mais informações.)
4. No PuTTYgen, selecione **Conversions** (Conversões) → **Export OpenSSH Key** (Exportar chave do OpenSSH) para exportar a chave privada. Não defina uma senha. Dê, à chave privada, o nome `PCPrivate.pem`.
5. Conecte-se ao comutador via Telnet ou SSH usando a autenticação por nome de usuário/senha.
6. Entre no modo de configuração:

   **`configure`**
7. Desative a transferência de arquivos por SSH:

   **`no ip ssh filetransfer`**
8. Habilite o cliente TFTP:

   **`tftp client`**
9. Mova a chave pública para o comutador:

   **`copy tftp pub-key-file`** ***<ip_servidor_tftp> <arquivo_de_chave_pública>*** **`manager`**
10. Habilite a autenticação de chave pública:

    **`aaa authentication ssh login public-key`**
11. Habilite a autenticação por usuário/senha:

    **`aaa authentication ssh enable local`**
12. Grave a configuração e a chave pública na memória:

    **`wr mem`**

## Criar uma credencial de protocolo SSH no Insight RS Console

Para configurar o SSH no Insight RS Console, conclua as seguintes etapas:

1. No Insight RS Console, adicione uma credencial de certificado SSH na guia **Detecção** → **Credenciais**.
   a. Na lista suspensa **Selecionar e configurar protocolo**, selecione **Secure Shell (SSH)** e clique em **Novo**.
   b. Na lista suspensa **Tipo**, selecione **Credencial de certificado**.
   c. Navegue até o arquivo da chave privada, `PCPrivate.pem`.
   d. Digite o alias do certificado. O alias assumirá a forma *nomedocomutador*-manager. O protocolo

SSH usa a porção *-manager* do alias como nome de usuário durante o logon.

2. Clique em **Adicionar**.

# Definir configurações de firewall e porta

Para obter uma lista completa de requisitos de firewall e de porta para dispositivos monitorados, consulte o *Informe de Segurança do HP Insight Remote Support*, em: http://www.hp.com/go/insightremotesupport/docs.

# Adicionar credenciais de protocolo e iniciar a detecção

Para detectar seus dispositivos monitorados, conclua as seguintes seções:

## Criar uma credencial de protocolo SNMP no Insight RS Console

Crie uma credencial de protocolo SNMP para a versão do SNMP que você configurou no comutador:

## Criar uma credencial de protocolo SNMPv1/v2 no Insight RS Console

Se a cadeia da comunidade SNMPv1 do dispositivo estiver definida como `pública` e o modo de acesso da comunidade for `somente leitura`, o Insight RS associará automaticamente um protocolo SNMP ao seu dispositivo. Se você usar uma cadeia de comunidade diferente ou uma porta não padrão, precisará criar uma credencial de protocolo SNMPv1 no Insight RS Console.

Para configurar o SNMPv1/v2 no Insight RS Console, conclua as seguintes etapas:

1. Em um navegador da Web, faça logon no Insight RS Console.
2. No menu principal, selecione **Detecção** e clique na guia **Credenciais**.
3. Na lista suspensa Selecionar e configurar protocolo, selecione **Simple Network Management Protocol versão 1 (SNMPv1)** ou **Simple Network Management Protocol versão 2 (SNMPv2)**.
4. Clique em **Novo**. A caixa de diálogo Nova credencial é exibida.
5. Digite a cadeia de caracteres da comunidade configurada no seu dispositivo.
6. Clique em **Adicionar**.

O Insight RS cria a credencial de protocolo, que é exibida na tabela de credenciais.

## Criar uma credencial de protocolo SNMPv3 no Insight RS

Crie uma credencial de protocolo SNMPv3 no Insight RS Console para que o Insight RS possa se comunicar com o seu dispositivo.

Para configurar o SNMPv3 no Insight RS Console, conclua as seguintes etapas:

1. Em um navegador da Web, faça logon no Insight RS Console.
2. No menu principal, selecione **Detecção** e clique na guia **Credenciais**.
3. Na lista suspensa Selecionar e configurar protocolo, selecione **Simple Network Management Protocol versão 3 (SNMPv3)**.
4. Clique em **Novo**. A caixa de diálogo Nova credencial é exibida.
5. Digite as seguintes informações necessárias:
   - **Protocolo de autenticação de conta**: `MD5` ou `SHA`
   - **Protocolo de privacidade de conta**: `DES, DES3, AES128, AES192, AES256`
   - **Senha de privacidade de conta**
   - **Nome de contexto**
6. Clique em **Adicionar**.

O Insight RS cria a credencial de protocolo, que é exibida na tabela de credenciais.

## Detectar o dispositivo no Insight RS Console

Para detectar o dispositivo por meio do Insight RS Console, conclua as seguintes etapas:

1. Em um navegador da Web, faça logon no Insight RS Console.
2. No menu principal, selecione **Detecção** e clique na guia **Fontes**.
3. Expanda a seção Endereços IP e adicione o endereço IP do seu dispositivo:
   a. Clique em **Novo**.
   b. Selecione **Endereço único**, **Intervalo de endereços** ou **Lista de endereços**.
   c. Digite os endereços IP dos dispositivos a serem detectados.
   d. Clique em **Adicionar**.
4. Clique em **Iniciar detecção**.

## Verificar o status de detecção e do dispositivo

Para verificar se o dispositivo foi detectado corretamente, conclua as seguintes etapas:

1. Em um navegador da Web, faça logon no Insight RS Console.
2. No menu principal, selecione **Dispositivos** e clique na guia **Resumo do dispositivo**.
3. Verifique se a coluna Status contém um ícone de êxito ( ).

   Se não houver ícone de êxito, tente descobrir que coluna está com problema e consulte a Ajuda on-line para informações de solução de problemas.

# Verificar a comunicação entre o dispositivo monitorado e o Insight RS

Para verificar a comunicação entre o dispositivo monitorado e o Insight RS, conclua a seguinte seção:

## Verificar coletas no Insight RS Console

Coletas não são executadas automaticamente depois da descoberta. A HP recomenda que você execute uma coleta manualmente após a descoberta completa para verificar a conectividade. Execute o cronograma de coleta manualmente na guia Serviços de coleta → Agendamentos de coleta. Para obter mais informações sobre o agendamento de coletas, consulte a Ajuda do Insight RS.

Verifique se essa coleta foi bem-sucedida na guia Serviços de coleta → Resultados da coleta básica do Insight RS Console.

1. Faça logon no Insight RS Console.
2. No menu principal, selecione **Serviços de coleta** e depois clique na guia **Resultados da coleta básica**.

3. Expanda a seção Coleta de configurações de rede.
4. Localize a entrada referente ao seu dispositivo e verifique a coluna Resultado. Se a coleta tiver sido bem-sucedida, um ícone de êxito será exibido (). Se ocorrer uma falha, um ícone de erro será exibido ().

# Capítulo 35: Configurar comutadores de rede baseados no Comware

Comutadores de rede baseados em Comware (os antigos comutadores da série A ou h4C/3COM) exigem o SNMP para detecção e monitoramento de eventos.

## Suporte à IRF (Intelligent Resilient Framework)

O Insight RS oferece suporte à tecnologia IRF (Intelligent Resilient Framework) e pode detectar os seguintes alertas IRF:

- Falha na fonte de alimentação
- Falhas em ventiladores e bandejas de ventiladores
- Falhas em módulos e placas
- Condições de excesso de temperatura

O Insight RS só detecta o comutador principal em uma pilha IRF, e o restante dos comutadores na pilha são identificados por meio das informações MIB. Após a construção da pilha IRF, o endereço IP do comutador principal torna-se um IP virtual (VIP). O VIP permanece estável mesmo quando a função de membro principal muda para um comutador membro diferente devido a uma falha no comutador principal. Se o comutador principal falhar, um novo membro principal assumirá seu lugar, e a configuração da pilha será identificado por meio da atualização MIB.

Quando o Insight RS descobrir a pilha IRF, será criado um Objeto de serviço (OOS) contendo as credenciais do comutador mestre no momento da detecção. Quando um evento é enviado à HP, essas credenciais são verificados quanto aos direitos, mas, mesmo que o membro principal tenha feito failover para um comutador membro IRF desconhecido (mas com direitos) e o número de série desse membro principal tenha mudado por conta disso, o OOS não mudará, a menos que tenha havido uma redescoberta de intervenção do IRF.

No entanto, para atender às verificações de direitos no Insight RS, a HP recomenda que, antes de uma pilha IRF ser construída, cada comutador seja individualmente descoberto para verificar se ele tem uma garantia ou contrato válido e está qualificado para suporte remoto. Isso impede o cenário em que o comutador faz failover para um comutador que não tem uma garantia ou contrato válido e, portanto, não está qualificado para suporte remoto. Se o novo membro principal não for qualificado, a pilha inteira IRF se tornará desqualificada. Se você não quer desmontar uma pilha existente, certifique-se de que todos os comutadores membros tenham uma garantia ou contrato válido.

**Importante:** Verifique se todos os comutadores membros da pilha IRF têm uma garantia ou contrato válido. Se o comutador principal falhar, o comutador membro designado para ser o novo comutador principal também deverá ter uma garantia ou contrato válido na pilha para continuar a ter direito ao suporte remoto. Se a pilha ainda não tiver sido construída, você poderá verificar o direito detectando cada comutador individualmente. Se a pilha já tiver sido construída, você deverá verificar manualmente se cada comutador tem uma garantia ou um contrato válido.

# Atender aos requisitos de configuração

Para configurar seus comutadores de rede baseados no Comware de forma que eles sejam monitorados pelo Insight RS, conclua as seguintes seções:

**Tabela 35.1** ***Etapas de configuração de comutadores de rede baseados no Comware***

| Tarefa | Concluída? |
|---|---|
| Verifique se o Insight RS oferece suporte ao seu comutador baseado em Comware, consultando as *Notas de Lançamento do HP Insight Remote Support*. | |
| Configure Telnet ou SSH no comutador. | |
| Configure as interceptações SNMP no comutador. | |
| Adicione credenciais de protocolo SNMP ao Insight RS Console para monitoramento. | |
| Adicione credenciais de protocolo Telnet ou SSH ao Insight RS Console para coletas. | |
| Detecte o comutador baseado em Comware no Insight RS Console. | |
| Verifique a comunicação por SNMP. | |

# Instalar e configurar o software de comunicação em comutadores

Para configurar seus dispositivos monitorados, conclua as seguintes seções:

## Configurar Telnet ou SSH

Para configurar destinos de interceptação para que apontem para o Insight Remote Support, você terá que usar Telnet ou SSH (ou um console serial) para acessar a CLI. Você também precisa configurar o Telnet ou SSH para permitir serviços de coleta. Use os procedimentos abaixo para configurar o Telnet ou SSH.

### *Configurar a Telnet*

Em um console serial, siga estas instruções:

1. Entre na visualização do sistema e ative o serviço Telnet.

   ```
   <Sysname> system-view [Sysname] telnet server enable
   ```

2. Configure um endereço IP para a interface VLAN 1. Esse endereço atuará como destino da conexão Telnet.

   ```
   [Switch] interface vlan-interface 1 [Switch-Vlan-interface1] ip address <ip_address> 255.255.255.0 [Switch-Vlan-interface1] quit
   ```

3. Defina o modo de autenticação das interfaces de usuário para o AAA.

   ```
   [Switch] user-interface vty 0 4 [Switch-ui-vty0-4] authentication-mode scheme
   ```

4. Ative o suporte a Telnet nas interfaces de usuário.

   ```
   [Switch-ui-vty0-4] protocol inbound telnet [Switch-ui-vty0-4] quit
   ```

5. Crie um usuário local `manager` e defina o nível de privilégios de comandos do usuário como 3

   ```
   [Switch] local-user manager [Switch-luser-client001] password simple <password>
   [Switch-luser-client001] service-type telnet [Switch-luser-client001]
   authorization-attribute level 3 [Switch-luser-client001] quit
   ```

## Configurar o SSH Versão 2

Em um console serial, siga estas instruções:

1. `<Switch> system-view [Switch] public-key local create rsa [Switch] public-key local create dsa [Switch] ssh server enable`

2. Configure um endereço IP para a interface VLAN 1. Esse endereço atuará como destino da conexão SSH.

   ```
   [Switch] interface vlan-interface 1 [Switch-Vlan-interface1] ip address <ip_
   address> 255.255.255.0 [Switch-Vlan-interface1] quit
   ```

3. Defina o modo de autenticação das interfaces de usuário para o AAA.

   ```
   [Switch] user-interface vty 0 4 [Switch-ui-vty0-4] authentication-mode scheme
   ```

4. Ative o suporte a SSH nas interfaces de usuário.

   ```
   [Switch-ui-vty0-4] protocol inbound ssh [Switch-ui-vty0-4] quit
   ```

5. Crie um usuário local `manager` e defina o nível de privilégios de comandos do usuário como 3.

   ```
   [Switch] local-user manager [Switch-luser-client001] password simple <password>
   [Switch-luser-client001] service-type ssh [Switch-luser-client001] authorization-
   attribute level 3 [Switch-luser-client001] quit
   ```

## Verificar a comunicação por Telnet/SSH

Para verificar se a comunicação por Telnet ou SSH está funcionando corretamente, conclua as seguintes etapas:

1. No dispositivo host, conecte-se ao comutador baseado em Comware usando o protocolo que você deseja verificar. Aguarde até que a conexão seja estabelecida.
2. Informe o `username` (nome de usuário) e a `password` (senha) quando solicitado.

   Um logon bem-sucedido confirma que o Telnet/SSH está configurado corretamente.

# Configurar interceptações SNMP

Comutadores de rede baseados no Comware podem ser configurados para usar SNMPv1, SNMPv2 ou SNMPv3. Selecione um dos métodos abaixo:

## Configurar o SNMPv1/v2

A partir de um console serial, ou através de SSH ou Telnet, siga estas instruções:

1. `<Sysname> system-view [Sysname] snmp-agent sys-info version v1 [Sysname] snmp-agent community read public`
2. Habilite as interceptações SNMP e defina o dispositivo host como destino da interceptação. Use `public` para o nome da comunidade.

   `[Sysname] snmp-agent trap enable [Sysname] snmp-agent target-host trap address udp-domain <hosting_device_ip> params securityname public v1`

## Salvar a configuração atual

Em um console serial, siga estas instruções:

1. Salve as alterações em sua configuração, emitindo o comando **save**.
2. Quando surgir a mensagem "a configuração atual será gravada no dispositivo", digite **Y**.
3. Pressione **Enter** para manter o nome de arquivo existente inalterado.
4. Ao ser solicitado para substituir o arquivo `*.cfg` existente, digite **Y**.

Uma mensagem de confirmação é exibida se a configuração atual for salva com sucesso.

## Configurar o SNMPv3

A partir de um console serial, ou através de SSH ou Telnet, siga estas instruções:

1. Entre na exibição do sistema:

   `system-view`
2. Habilite o agente SNMP:

   `snmp-agent`
3. Configure um grupo SNMP e especifique seu direito de acesso:

   `snmp-agent group v3 <group-name> [authentication | privacy] [read-view <read-view>] [write-view <write-view>] [notify-view <notify-view>] [acl <acl-number>]`
4. Adicione um usuário ao grupo SNMP:

```
snmp-agent usm-user v3 <user-name> <group-name> [[cipher] authentication-mode {md5
| sha} <auth-password> [privacy-mode {3des | aes128 | des56} <priv-password>]]
[acl <acl-number>]
```

O valor de **auth-password** precisa ter pelo menos 6 caracteres para o Insight RS.

5. Habilite as interceptações SNMP e defina o dispositivo host como destino da interceptação:

```
[Sysname] snmp-agent trap enable
[Sysname] snmp-agent target-host trap address udp-domain <hosting-device-ip>
params securityname <security-string> v3
```

### *Salvar a configuração atual*

Em um console serial, siga estas instruções:

1. Salve as alterações em sua configuração, emitindo o comando **save**.
2. Quando surgir a mensagem "a configuração atual será gravada no dispositivo", digite **Y**.
3. Pressione **Enter** para manter o nome de arquivo existente inalterado.
4. Ao ser solicitado para substituir o arquivo `*.cfg` existente, digite **Y**.

Uma mensagem de confirmação é exibida se a configuração atual for salva com sucesso.

## Definir configurações de firewall e porta

Para obter uma lista completa de requisitos de firewall e de porta para dispositivos monitorados, consulte o *Informe de Segurança do HP Insight Remote Support*, em: http://www.hp.com/go/insightremotesupport/docs.

# Adicionar credenciais de protocolo e iniciar a detecção

Para detectar seus dispositivos monitorados, conclua as seguintes seções:

## Criar uma credencial de protocolo SNMP no Insight RS Console

Crie uma credencial de protocolo SNMP para a versão do SNMP que você configurou no comutador:

### *Criar uma credencial de protocolo SNMPv1/v2 no Insight RS Console*

Se a cadeia da comunidade SNMPv1 do dispositivo estiver definida como `pública` e o modo de acesso da comunidade for `somente leitura`, o Insight RS associará automaticamente um protocolo SNMP ao seu dispositivo. Se você usar uma cadeia de comunidade diferente ou uma porta não padrão, precisará criar uma credencial de protocolo SNMPv1 no Insight RS Console.

Para configurar o SNMPv1/v2 no Insight RS Console, conclua as seguintes etapas:

1. Em um navegador da Web, faça logon no Insight RS Console.
2. No menu principal, selecione **Detecção** e clique na guia **Credenciais**.
3. Na lista suspensa Selecionar e configurar protocolo, selecione **Simple Network Management Protocol versão 1 (SNMPv1)** ou **Simple Network Management Protocol versão 2 (SNMPv2)**.
4. Clique em **Novo**. A caixa de diálogo Nova credencial é exibida.
5. Digite a cadeia de caracteres da comunidade configurada no seu dispositivo.
6. Clique em **Adicionar**.

O Insight RS cria a credencial de protocolo, que é exibida na tabela de credenciais.

## *Criar uma credencial de protocolo SNMPv3 no Insight RS*

Crie uma credencial de protocolo SNMPv3 no Insight RS Console para que o Insight RS possa se comunicar com o seu dispositivo.

Para configurar o SNMPv3 no Insight RS Console, conclua as seguintes etapas:

1. Em um navegador da Web, faça logon no Insight RS Console.
2. No menu principal, selecione **Detecção** e clique na guia **Credenciais**.
3. Na lista suspensa Selecionar e configurar protocolo, selecione **Simple Network Management Protocol versão 3 (SNMPv3)**.
4. Clique em **Novo**. A caixa de diálogo Nova credencial é exibida.
5. Digite as seguintes informações necessárias:
   - **Protocolo de autenticação de conta**: `MD5` ou `SHA`
   - **Protocolo de privacidade de conta**: `DES, DES3, AES128, AES192, AES256`
   - **Senha de privacidade de conta**
   - **Nome de contexto**
6. Clique em **Adicionar**.

O Insight RS cria a credencial de protocolo, que é exibida na tabela de credenciais.

# Criar um protocolo Telnet ou SSH no Insight RS Console

Crie uma credencial de protocolo Telnet ou SSH no Insight RS Console. Você não precisa configurar ambos.

## *Criar um protocolo Telnet no Insight RS Console*

Para configurar o Telnet no Insight RS Console, conclua as seguintes etapas:

1. Em um navegador da Web, faça logon no Insight RS Console.
2. No menu principal, selecione **Detecção** e clique na guia **Credenciais**.
3. Na lista suspensa **Selecionar e configurar protocolo**, selecione **Telnet**.
4. Clique em **Novo**. A caixa de diálogo Nova credencial é exibida.

O Insight RS cria a credencial de protocolo, que é exibida na tabela de credenciais.

### *Criar uma credencial de protocolo SSH no Insight RS Console*

Para configurar o SSH no Insight RS Console, conclua as seguintes etapas:

1. Em um navegador da Web, faça logon no Insight RS Console.
2. No menu principal, selecione **Detecção** e clique na guia **Credenciais**.
3. Na lista suspensa **Selecionar e configurar protocolo**, selecione **Secure Shell (SSH)**.
4. Clique em **Novo**. A caixa de diálogo Nova credencial é exibida.
5. Digite o nome de usuário e a senha configurados no seu dispositivo.
6. Clique em **Adicionar**.

O Insight RS cria a credencial de protocolo, que é exibida na tabela de credenciais.

## Detectar o dispositivo no Insight RS Console

**Importante:** O ICMP é usado pelo Insight RS para detecção. Verifique se o ICMP está habilitado no seu dispositivo.

Para detectar o dispositivo por meio do Insight RS Console, conclua as seguintes etapas:

1. Em um navegador da Web, faça logon no Insight RS Console.
2. No menu principal, selecione **Detecção** e clique na guia **Fontes**.
3. Expanda a seção Endereços IP e adicione o endereço IP do seu dispositivo:
   a. Clique em **Novo**.
   b. Selecione **Endereço único**, **Intervalo de endereços** ou **Lista de endereços**.
   c. Digite os endereços IP dos dispositivos a serem detectados.
   d. Clique em **Adicionar**.
4. Clique em **Iniciar detecção**.

## Verificar o status de detecção e do dispositivo

Para verificar se o dispositivo foi detectado corretamente, conclua as seguintes etapas:

1. Em um navegador da Web, faça logon no Insight RS Console.
2. No menu principal, selecione **Dispositivos** e clique na guia **Resumo do dispositivo**.
3. Verifique se a coluna Status contém um ícone de êxito (✅).

   Se não houver ícone de êxito, tente descobrir que coluna está com problema e consulte a Ajuda on-line para informações de solução de problemas.

# Verificar informações de garantia e contrato

Verifique se as informações de garantia e contrato foram detectadas corretamente no Insight RS Console:

1. No Insight RS Console, navegue até **Dispositivos** e clique na opção Nome do dispositivo.
2. Expanda a seção Hardware e confira se o **Número de série adquirido** e o **Número do produto adquirido** estão corretos. Se eles não estiverem corretos, digite os valores corretos nos campos **Substituir número de série** e **Substituir número do produto** e clique em **Salvar alterações**.

# Verificar a comunicação entre o dispositivo monitorado e o Insight RS

Para verificar a comunicação entre o dispositivo monitorado e o Insight RS, conclua as seguintes seções:

## Verificar a comunicação por SNMP

Não há como verificar manualmente a configuração do SNMP sem gerar um evento, e, para isso, é necessário fazer algo como remover uma bandeja de ventilador ou desconectar uma fonte de alimentação.

**Observação:** Não puxe uma FRU redundante para testar a configuração.

Você pode verificar a comunicação SNMP revendo a configuração em execução na linha de comando do comutador baseado em ComWare. Procure a seção `snmp-agent` na saída e verifique se a cadeia de caracteres de "community" está correta e o destino da interceptação é o dispositivo host.

Para mostrar a configuração em execução, execute o seguinte comando:

```
> display current-configuration
```

```
# snmp-agent snmp-agent community read public snmp-agent sys-info version v1 snmp-agent target-host trap address udp-domain <hosting_device_ip> params securityname public v1 #
```

Se qualquer uma das configurações estiver incorreta, use o comando **undo** para remover a configuração, como **`undo snmp-agent community read public`**. Em seguida, volte para "Configurar interceptações SNMP", e reconfigure o que estava incorreto.

# Verificar coletas no Insight RS Console

Coletas não são executadas automaticamente depois da descoberta. A HP recomenda que você execute uma coleta manualmente após a descoberta completa para verificar a conectividade. Execute o cronograma de coleta manualmente na guia Serviços de coleta → Agendamentos de coleta. Para obter mais informações sobre o agendamento de coletas, consulte a Ajuda do Insight RS.

Verifique se essa coleta foi bem-sucedida na guia Serviços de coleta → Resultados da coleta básica do Insight RS Console.

1. Faça logon no Insight RS Console.
2. No menu principal, selecione **Serviços de coleta** e depois clique na guia **Resultados da coleta básica**.
3. Expanda a seção Coleta de configurações de rede.
4. Localize a entrada referente ao seu dispositivo e verifique a coluna Resultado. Se a coleta tiver sido bem-sucedida, um ícone de êxito será exibido ( ). Se ocorrer uma falha, um ícone de erro será exibido ( ).

# Capítulo 36: Configurar comutadores Mellanox InfiniBand

Comutadores InfiniBand exigem o SNMP para descoberta, monitoramento de eventos e coletas.

## Atender aos requisitos de configuração

Para configurar comutadores InfiniBand de forma que eles sejam monitorados pelo Insight RS, conclua as seguintes seções:

**Tabela 36.1** ***Etapas de configuração do comutador InfiniBand***

| Tarefa | Concluída? |
| --- | --- |
| Certifique-se de que o Insight RS ofereça suporte ao seu comutador InfiniBand, verificando o documento *Notas de Lançamento do HP Insight Remote Support*. | |
| Configure as interceptações SNMP no comutador. | |
| Adicione credenciais de protocolo SNMP ao Insight RS Console para monitoramento. | |
| Detecte o comutador InfiniBand no Insight RS Console. | |
| Verifique a comunicação por SNMP. | |

## Instalar e configurar o software de comunicação em comutadores

Para configurar seus dispositivos monitorados, conclua as seguintes seções:

## Configurar interceptações SNMP

Comutadores InfiniBand podem ser configurados para usar SNMPv1, SNMPv2 ou SNMPv3. Selecione um dos métodos abaixo:

### *Configurar o SNMPv1/v2*

Em um console, siga estas instruções:

1. Ative o servidor SNMP no comutador (no modo de configuração) usando os seguintes comandos:

```
switch (config) # snmp-server enable
switch (config) # snmp-server enable notify
switch (config) # snmp-server community public ro
switch (config) # snmp-server contact "nome do contato"
switch (config) # snmp-server host <endereço_IP_dispositivo_host> traps version 2c
public
switch (config) # snmp-server location "nome do local"
switch (config) # snmp-server user admin v3 enable
switch (config) # snmp-server user admin v3 prompt auth md5 priv des
```

2. Habilite o SNMP SET para permitir operações SET SNMP usando SNMPv1/v2:
   a. Habilite comunidades SNMP:
      ```
      switch (config) # snmp-server enable communities
      ```
   b. Configure uma comunidade de leitura/gravação:
      ```
      switch (config) # snmp-server community my-community-name rw
      ```
   c. Certifique-se de que comunidades SNMP estejam habilitadas. Verifique se a indicação "(DISABLED)" não aparece ao lado de "Read-only communities"/"Read-write communities".
      ```
      switch (config) # show snmp
      ```

## Configurar o SNMPv3

Em um console, siga estas instruções:

1. Configure um usuário SNMPv3:
   a. Configure o usuário:
      ```
      switch (config) # snmp-server user admin v3 prompt auth <tipo de hash> priv
      <tipo de privacidade>
      ```
      em que o *tipo de hash* pode ser igual a `md5` ou `sha`, enquanto o *tipo de privacidade* pode ser igual a `des` ou `aes-128`.
   b. Insira a senha de autenticação e sua confirmação.
   c. Insira a senha de privacidade e sua confirmação.
2. Configure as interceptações de Notificação SNMP:
   a. Verifique se as notificações SNMP e SNMP estão habilitadas:
      ```
      switch (config) # snmp-server enable
      switch (config) # snmp-server enable notify
      ```
   b. Configure o host SNMP:
      ```
      switch (config) # snmp-server host <endereço_IP_dispositivo_host> traps version
      3 user <nomeusuário> auth sha <senha>
      ```
   c. Verifique a configuração do host SNMP.
      ```
      switch (config) # show snmp host
      ```
3. Habilite o SNMP SET para permitir operações SET SNMP usando SNMPv3:
   a. Crie um usuário SNMPv3:
      ```
      switch (config) # snmp-server user <usuário> v3 auth sha <senha1> priv aes-128
      <senha2>
      ```
   b. Verifique se o nome de usuário está habilitado para acesso SET e tem o nível de capacidade admin:
      ```
      switch (config) # show snmp user
      ```

# Definir configurações de firewall e porta

Para obter uma lista completa de requisitos de firewall e de porta para dispositivos monitorados, consulte o *Informe de Segurança do HP Insight Remote Support*, em: http://www.hp.com/go/insightremotesupport/docs.

# Adicionar credenciais de protocolo e iniciar a detecção

Para detectar seus dispositivos monitorados, conclua as seguintes seções:

# Criar uma credencial de protocolo SNMP no Insight RS Console

Crie uma credencial de protocolo SNMP para a versão do SNMP que você configurou no comutador:

## *Criar uma credencial de protocolo SNMPv1/v2 no Insight RS Console*

Se a cadeia da comunidade SNMPv1 do dispositivo estiver definida como `pública` e o modo de acesso da comunidade for `somente leitura`, o Insight RS associará automaticamente um protocolo SNMP ao seu dispositivo. Se você usar uma cadeia de comunidade diferente ou uma porta não padrão, precisará criar uma credencial de protocolo SNMPv1 no Insight RS Console.

Para configurar o SNMPv1/v2 no Insight RS Console, conclua as seguintes etapas:

1. Em um navegador da Web, faça logon no Insight RS Console.
2. No menu principal, selecione **Detecção** e clique na guia **Credenciais**.
3. Na lista suspensa Selecionar e configurar protocolo, selecione **Simple Network Management Protocol versão 1 (SNMPv1)** ou **Simple Network Management Protocol versão 2 (SNMPv2)**.
4. Clique em **Novo**. A caixa de diálogo Nova credencial é exibida.
5. Digite a cadeia de caracteres da comunidade configurada no seu dispositivo.
6. Clique em **Adicionar**.

O Insight RS cria a credencial de protocolo, que é exibida na tabela de credenciais.

## *Criar uma credencial de protocolo SNMPv3 no Insight RS*

Crie uma credencial de protocolo SNMPv3 no Insight RS Console para que o Insight RS possa se comunicar com o seu dispositivo.

Para configurar o SNMPv3 no Insight RS Console, conclua as seguintes etapas:

1. Em um navegador da Web, faça logon no Insight RS Console.
2. No menu principal, selecione **Detecção** e clique na guia **Credenciais**.

3. Na lista suspensa Selecionar e configurar protocolo, selecione **Simple Network Management Protocol versão 3 (SNMPv3)**.
4. Clique em **Novo**. A caixa de diálogo Nova credencial é exibida.
5. Digite as seguintes informações necessárias:
   - **Protocolo de autenticação de conta**: `MD5` ou `SHA`
   - **Protocolo de privacidade de conta**: `DES, DES3, AES128, AES192, AES256`
   - **Senha de privacidade de conta**
   - **Nome de contexto**
6. Clique em **Adicionar**.

O Insight RS cria a credencial de protocolo, que é exibida na tabela de credenciais.

# Detecte o dispositivo no Insight RS Console

**Importante:** O ICMP é usado pelo Insight RS para detecção. Verifique se o ICMP está habilitado no seu dispositivo.

Para detectar o dispositivo por meio do Insight RS Console, siga estas instruções:

1. Em um navegador da Web, faça logon no Insight RS Console.
2. No menu principal, selecione **Detecção** e clique na guia **Fontes**.
3. Expanda a seção Endereços IP e adicione o endereço IP do seu dispositivo:
   a. Clique em **Novo**.
   b. Selecione **Endereço único**, **Intervalo de endereços** ou **Lista de endereços**.
   c. Digite os endereços IP dos dispositivos a serem detectados.
   d. Clique em **Adicionar**.
4. Clique em **Iniciar detecção**.

# Verificar o status de detecção e do dispositivo

Para verificar se o dispositivo foi detectado corretamente, conclua as seguintes etapas:

1. Em um navegador da Web, faça logon no Insight RS Console.
2. No menu principal, selecione **Dispositivos** e clique na guia **Resumo do dispositivo**.
3. Verifique se a coluna Status contém um ícone de êxito ( ).

   Se não houver ícone de êxito, tente descobrir que coluna está com problema e consulte a Ajuda on-line para informações de solução de problemas.

# Verificar a comunicação entre o dispositivo monitorado e o Insight RS

Para verificar a comunicação entre o dispositivo monitorado e o Insight RS, conclua as seguintes seções:

## Verificar a comunicação por SNMP

Verifique se o SNMP está se comunicando com o dispositivo host, enviando uma solicitação SET de interceptação de teste:

1. Envie uma solicitação SET ao IP do comutador com o OID 1.3.6.1.4.1.33049.2.1.1.1.6.0.
2. Certifique-se de que a interceptação de teste seja recebida pelo receptor de interceptações (OID: 1.3.6.1.4.1.33049.2.1.2.13).

## Verificar coletas no Insight RS Console

Coletas não são executadas automaticamente depois da descoberta. A HP recomenda que você execute uma coleta manualmente após a descoberta completa para verificar a conectividade. Execute o cronograma de coleta manualmente na guia Serviços de coleta → Agendamentos de coleta. Para obter mais informações sobre o agendamento de coletas, consulte a Ajuda do Insight RS.

Verifique se essa coleta foi bem-sucedida na guia Serviços de coleta → Resultados da coleta básica do Insight RS Console.

1. Faça logon no Insight RS Console.
2. No menu principal, selecione **Serviços de coleta** e depois clique na guia **Resultados da coleta básica**.
3. Expanda a seção Coleta de configurações de rede.
4. Localize a entrada referente ao seu dispositivo e verifique a coluna Resultado. Se a coleta tiver sido bem-sucedida, um ícone de êxito será exibido (). Se ocorrer uma falha, um ícone de erro será exibido ().

# Capítulo 37: Configurar roteadores de rede

Roteadores de rede da HP exigem o SNMP para o monitoramento de eventos e o Telnet/SSH para coletas.

## Atender aos requisitos de configuração

Para configurar roteadores de forma que eles sejam monitorados pelo Insight RS, conclua as seguintes seções:

**Tabela 37.1** ***Etapas de configuração do roteador de rede***

| Tarefa | Concluída? |
|---|---|
| Certifique-se de que o Insight RS ofereça suporte ao seu roteador, verificando o *Notas de Lançamento do HP Insight Remote Support*. | |
| Configure o Telnet ou o SSH no roteador. | |
| Configure interceptações SNMP no roteador. | |
| Adicione credenciais de protocolo SNMP ao Insight RS Console para monitoramento. | |
| Adicione credenciais de protocolo Telnet ou SSH ao Insight RS Console para coletas. | |
| Detecte o roteador no Insight RS Console. | |
| Verifique a comunicação por SNMP. | |

## Instalar e configurar o software de comunicação em roteadores

Para configurar seus dispositivos monitorados, conclua as seguintes seções:

## Configurar Telnet ou SSH

Para configurar destinos de interceptação para que apontem para o Insight Remote Support, você terá que usar Telnet ou SSH (ou um console serial) para acessar a CLI. Você também precisa configurar o Telnet ou SSH para permitir serviços de coleta. Use os procedimentos abaixo para configurar o Telnet ou SSH.

### *Configurar a Telnet*

Em um console serial, siga estas instruções:

1. Entre na visualização do sistema e ative o serviço Telnet.

   ```
   <Sysname> system-view [Sysname] telnet server enable
   ```

2. Configure um endereço IP para a interface VLAN 1. Esse endereço atuará como destino da conexão Telnet.

```
[Sysname] interface vlan-interface 1 [Sysname-Vlan-interface1] ip address <ip-address> 255.255.255.0 [Sysname-Vlan-interface1] quit
```

3. Defina o modo de autenticação das interfaces de usuário para o AAA.

   ```
   [Sysname] user-interface vty 0 4 [Sysname-ui-vty0-4] authentication-mode scheme
   ```

4. Ative o suporte a Telnet nas interfaces de usuário.

   ```
   [Sysname-ui-vty0-4] protocol inbound telnet [Sysname-ui-vty0-4] quit
   ```

5. Crie um usuário local `manager` e defina o nível de privilégios de comandos do usuário como 3

   ```
   [Sysname] local-user manager [Sysname-luser-client001] password simple <password> [Sysname-luser-client001] service-type telnet [Sysname-luser-client001] authorization-attribute level 3 [Sysname-luser-client001] quit
   ```

## *Configurar o SSH Versão 2*

Em um console serial, siga estas instruções:

1. `<Sysname> system-view [Sysname] public-key local create rsa [Sysname] public-key local create dsa [Sysname] ssh server enable`

2. Configure um endereço IP para a interface VLAN 1. Esse endereço atuará como destino da conexão SSH.

   ```
   [Sysname] interface vlan-interface 1 [Sysname-Vlan-interface1] ip address <ip-address> 255.255.255.0 [Sysname-Vlan-interface1] quit
   ```

3. Defina o modo de autenticação das interfaces de usuário para o AAA.

   ```
   [Sysname] user-interface vty 0 4 [Sysname-ui-vty0-4] authentication-mode scheme
   ```

4. Ative o suporte a SSH nas interfaces de usuário.

   ```
   [Sysname-ui-vty0-4] protocol inbound ssh [Sysname-ui-vty0-4] quit
   ```

5. Crie um usuário local `manager` e defina o nível de privilégios de comandos do usuário como 3.

   ```
   [Sysname] local-user manager [Sysname-luser-client001] password simple <password> [Sysname-luser-client001] service-type ssh [Sysname-luser-client001] authorization-attribute level 3 [Sysname-luser-client001] quit
   ```

## Verificar a comunicação por Telnet/SSH

Para verificar se a comunicação por Telnet ou SSH está funcionando corretamente, conclua as seguintes etapas:

1. No dispositivo host, conecte-se ao roteador usando o protocolo que você deseja verificar. Aguarde até que a conexão seja estabelecida.
2. Informe o `username` (nome de usuário) e a `password` (senha) quando solicitado.

   Um logon bem-sucedido confirma que o Telnet/SSH está configurado corretamente.

# Configurar interceptações de SNMP

Roteadores de rede podem ser configurados para usar SNMPv1, SNMPv2 ou SNMPv3. Selecione um dos métodos abaixo:

## Configurar o SNMPv1/v2

A partir de um console serial, ou através de SSH ou Telnet, siga estas instruções:

1. **`<Sysname> system-view [Sysname] snmp-agent sys-info version v1 [Sysname] snmp-agent community read public`**
2. Habilite as interceptações SNMP e defina o dispositivo host como destino da interceptação. Use `public` para o nome da comunidade.

   **`[Sysname] snmp-agent trap enable [Sysname] snmp-agent target-host trap address udp-domain <hosting-device-ip> params securityname public v1`**

## Salvar a configuração atual

Em um console serial, siga estas instruções:

1. Salve as alterações em sua configuração, emitindo o comando **save**.
2. Quando surgir a mensagem "a configuração atual será gravada no dispositivo", digite **Y**.
3. Pressione **Enter** para manter o nome de arquivo existente inalterado.
4. Ao ser solicitado para substituir o arquivo `*.cfg` existente, digite **Y**.

Uma mensagem de confirmação é exibida se a configuração atual for salva com sucesso.

## Configurar o SNMPv3

A partir de um console serial, ou através de SSH ou Telnet, siga estas instruções:

1. Entre na exibição do sistema:

   ```
   system-view
   ```

2. Habilite o agente SNMP:

   ```
   snmp-agent
   ```

3. Configure um grupo SNMP e especifique seu direito de acesso:

   ```
   snmp-agent group v3 <group-name> [authentication | privacy] [read-view <read-view>] [write-view <write-view>] [notify-view <notify-view>] [acl <acl-number>]
   ```

4. Adicione um usuário ao grupo SNMP:

   ```
   snmp-agent usm-user v3 <user-name> <group-name> [[cipher] authentication-mode {md5 | sha} <auth-password> [privacy-mode {3des | aes128 | des56} <priv-password>]] [acl <acl-number>]
   ```

   O valor de **auth-password** precisa ter pelo menos 6 caracteres para o Insight RS.

5. Habilite as interceptações SNMP e defina o dispositivo host como destino da interceptação:

   ```
   [Sysname] snmp-agent trap enable
   [Sysname] snmp-agent target-host trap address udp-domain <hosting-device-ip> params securityname <security-string> v3
   ```

### *Salvar a configuração atual*

Em um console serial, siga estas instruções:

1. Salve as alterações em sua configuração, emitindo o comando **save**.
2. Quando surgir a mensagem "a configuração atual será gravada no dispositivo", digite **Y**.
3. Pressione **Enter** para manter o nome de arquivo existente inalterado.
4. Ao ser solicitado para substituir o arquivo `*.cfg` existente, digite **Y**.

Uma mensagem de confirmação é exibida se a configuração atual for salva com sucesso.

## Definir configurações de firewall e porta

Para obter uma lista completa de requisitos de firewall e de porta para dispositivos monitorados, consulte o *Informe de Segurança do HP Insight Remote Support*, em: http://www.hp.com/go/insightremotesupport/docs.

# Adicionar credenciais de protocolo e iniciar a detecção

Para detectar seus dispositivos monitorados, conclua as seguintes seções:

# Criar uma credencial de protocolo SNMP no Insight RS Console

Crie uma credencial de protocolo SNMP para a versão do SNMP que você configurou no roteador:

## *Criar uma credencial de protocolo SNMPv1/v2 no Insight RS Console*

Se a cadeia da comunidade SNMPv1 do dispositivo estiver definida como `pública` e o modo de acesso da comunidade for `somente leitura`, o Insight RS associará automaticamente um protocolo SNMP ao seu dispositivo. Se você usar uma cadeia de comunidade diferente ou uma porta não padrão, precisará criar uma credencial de protocolo SNMPv1 no Insight RS Console.

Para configurar o SNMPv1/v2 no Insight RS Console, conclua as seguintes etapas:

1. Em um navegador da Web, faça logon no Insight RS Console.
2. No menu principal, selecione **Detecção** e clique na guia **Credenciais**.
3. Na lista suspensa Selecionar e configurar protocolo, selecione **Simple Network Management Protocol versão 1 (SNMPv1)** ou **Simple Network Management Protocol versão 2 (SNMPv2)**.
4. Clique em **Novo**. A caixa de diálogo Nova credencial é exibida.
5. Digite a cadeia de caracteres da comunidade configurada no seu dispositivo.
6. Clique em **Adicionar**.

O Insight RS cria a credencial de protocolo, que é exibida na tabela de credenciais.

## *Criar uma credencial de protocolo SNMPv3 no Insight RS*

Crie uma credencial de protocolo SNMPv3 no Insight RS Console para que o Insight RS possa se comunicar com o seu dispositivo.

Para configurar o SNMPv3 no Insight RS Console, conclua as seguintes etapas:

1. Em um navegador da Web, faça logon no Insight RS Console.
2. No menu principal, selecione **Detecção** e clique na guia **Credenciais**.
3. Na lista suspensa Selecionar e configurar protocolo, selecione **Simple Network Management Protocol versão 3 (SNMPv3)**.
4. Clique em **Novo**. A caixa de diálogo Nova credencial é exibida.
5. Digite as seguintes informações necessárias:
   - **Protocolo de autenticação de conta**: `MD5` ou `SHA`
   - **Protocolo de privacidade de conta**: `DES, DES3, AES128, AES192, AES256`
   - **Senha de privacidade de conta**

- **Nome de contexto**

6. Clique em **Adicionar**.

O Insight RS cria a credencial de protocolo, que é exibida na tabela de credenciais.

# Criar um protocolo Telnet ou SSH no Insight RS Console

Crie uma credencial de protocolo Telnet ou SSH no Insight RS Console. Você não precisa configurar ambos.

## *Criar um protocolo Telnet no Insight RS Console*

Para configurar o Telnet no Insight RS Console, conclua as seguintes etapas:

1. Em um navegador da Web, faça logon no Insight RS Console.
2. No menu principal, selecione **Detecção** e clique na guia **Credenciais**.
3. Na lista suspensa **Selecionar e configurar protocolo**, selecione **Telnet**.
4. Clique em **Novo**. A caixa de diálogo Nova credencial é exibida.

O Insight RS cria a credencial de protocolo, que é exibida na tabela de credenciais.

## *Criar uma credencial de protocolo SSH no Insight RS Console*

Para configurar o SSH no Insight RS Console, conclua as seguintes etapas:

1. Em um navegador da Web, faça logon no Insight RS Console.
2. No menu principal, selecione **Detecção** e clique na guia **Credenciais**.
3. Na lista suspensa **Selecionar e configurar protocolo**, selecione **Secure Shell (SSH)**.
4. Clique em **Novo**. A caixa de diálogo Nova credencial é exibida.
5. Digite o nome de usuário e a senha configurados no seu dispositivo.
6. Clique em **Adicionar**.

O Insight RS cria a credencial de protocolo, que é exibida na tabela de credenciais.

# Detectar o dispositivo no Insight RS Console

**Importante:** O ICMP é usado pelo Insight RS para detecção. Verifique se o ICMP está habilitado no seu dispositivo.

Para detectar o dispositivo por meio do Insight RS Console, conclua as seguintes etapas:

1. Em um navegador da Web, faça logon no Insight RS Console.
2. No menu principal, selecione **Detecção** e clique na guia **Fontes**.

3. Expanda a seção Endereços IP e adicione o endereço IP do seu dispositivo:
   a. Clique em **Novo**.
   b. Selecione **Endereço único**, **Intervalo de endereços** ou **Lista de endereços**.
   c. Digite os endereços IP dos dispositivos a serem detectados.
   d. Clique em **Adicionar**.
4. Clique em **Iniciar detecção**.

# Verificar o status de detecção e do dispositivo

Para verificar se o dispositivo foi detectado corretamente, conclua as seguintes etapas:

1. Em um navegador da Web, faça logon no Insight RS Console.
2. No menu principal, selecione **Dispositivos** e clique na guia **Resumo do dispositivo**.
3. Verifique se a coluna Status contém um ícone de êxito (✅).

   Se não houver ícone de êxito, tente descobrir que coluna está com problema e consulte a Ajuda on-line para informações de solução de problemas.

# Verificar informações de garantia e contrato

Verifique se as informações de garantia e contrato foram detectadas corretamente no Insight RS Console:

1. No Insight RS Console, navegue até **Dispositivos** e clique no nome do dispositivo de roteador.
2. Expanda a seção Hardware e confira se o **Número de série adquirido** e o **Número do produto adquirido** estão corretos. Se eles não estiverem corretos, digite os valores corretos nos campos **Substituir número de série** e **Substituir número do produto** e clique em **Salvar alterações**.

# Verificar a comunicação entre o dispositivo monitorado e o Insight RS

Para verificar a comunicação entre o dispositivo monitorado e o Insight RS, conclua as seguintes seções:

# Verificar a comunicação por SNMP

Não há como verificar manualmente a configuração do SNMP sem gerar um evento, e, para isso, é necessário fazer algo como remover uma bandeja de ventilador ou desconectar uma fonte de alimentação.

**Observação:** Não puxe uma FRU redundante para testar a configuração.

Você pode verificar a comunicação SNMP revendo a configuração em execução na linha de comando do roteador. Procure a seção `snmp-agent` na saída e verifique se a cadeia de caracteres de "community" está correta e o destino da interceptação é o dispositivo host.

Para mostrar a configuração em execução, execute o seguinte comando:

```
> display current-configuration
```

```
# snmp-agent snmp-agent community read public snmp-agent sys-info version v1 snmp-
agent target-host trap address udp-domain <hosting_device_ip> params securityname
public v1 #
```

Se qualquer uma das configurações estiver incorreta, use o comando **undo** para remover a configuração, como **`undo snmp-agent community read public`**. Em seguida, volte para "Configurar roteadores de rede", e reconfigure o que estava incorreto.

# Verificar coletas no Insight RS Console

Coletas não são executadas automaticamente depois da descoberta. A HP recomenda que você execute uma coleta manualmente após a descoberta completa para verificar a conectividade. Execute o cronograma de coleta manualmente na guia Serviços de coleta → Agendamentos de coleta. Para obter mais informações sobre o agendamento de coletas, consulte a Ajuda do Insight RS.

Verifique se essa coleta foi bem-sucedida na guia Serviços de coleta → Resultados da coleta básica do Insight RS Console.

1. Faça logon no Insight RS Console.
2. No menu principal, selecione **Serviços de coleta** e depois clique na guia **Resultados da coleta básica**.
3. Expanda a seção Coleta de configurações de rede.
4. Localize a entrada referente ao seu dispositivo e verifique a coluna Resultado. Se a coleta tiver sido bem-sucedida, um ícone de êxito será exibido ( ). Se ocorrer uma falha, um ícone de erro será exibido ( ).

# Capítulo 38: Configurar sistemas de alimentação ininterrupta

Sistemas de alimentação ininterrupta (UPS) são fornecidos com um módulo de gerenciamento ou um módulo de rede instalado, dependendo do modelo. Use o procedimento de configuração apropriado abaixo para o seu modelo:

- Para configurar um UPS que usa um módulo de gerenciamento, consulte "Configurando módulos de gerenciamento UPS".
- Para configurar um UPS que usa um módulo de rede, consulte "Configurando módulos de rede UPS".

# Configurando módulos de gerenciamento UPS

O módulo de gerenciamento UPS ((No-break) é um componente opcional opção em várias unidades UPS montáveis em rack e de torre HP, e essas unidades podem ser monitoradas pelo Insight Remote Support nesse módulo.

**Importante:** Não há suporte para coletas de configuração.

## Atender aos requisitos de configuração

Para configurar módulos de gerenciamento UPS de forma que eles sejam monitorados pelo Insight RS, conclua as seguintes seções:

**Tabela 38.1** ***Etapas de configuração do módulo de gerenciamento UPS***

| Tarefa | Concluída? |
|---|---|
| Verifique se o Insight RS oferece suporte ao seu módulo de gerenciamento UPS, verificando o documento *Notas de Lançamento do HP Insight Remote Support*. | |
| Configure o SNMP no módulo de gerenciamento UPS e defina o dispositivo host como destinatário da interceptação. | |
| Adicione o protocolo SNMP ao Insight RS Console. | |
| Detecte o módulo de gerenciamento UPS no Insight RS Console. | |
| Envie um evento de teste para verificar a conectividade entre seu módulo de gerenciamento UPS e o Insight RS. | |

## Instalar e configurar o software de comunicação em módulos de gerenciamento

Para configurar seus dispositivos monitorados, conclua as seguintes seções:

### *Configurar o SNMP*

O SNMP pode ser configurado na tela Interceptações SNMP da interface da Web do módulo de gerenciamento UPS.

Para mais detalhes sobre configurar o SNMP, consulte o *Guia do usuário do módulo de gerenciamento UPS HP*.

Para configurar notificações de interceptação SNMP, conclua as seguintes etapas:

1. Faça logon na interface da web do módulo de gerenciamento UPS.
2. Clique na guia **Configuração** e, no menu à esquerda, clique em **Notificações de eventos**.
3. Adicione o dispositivo host do Insight RS como um destinatário de interceptação SNMP na guia Interceptações SNMP.
   a. Clique na guia **Interceptações SNMP**. Essa tela permite que os administradores configurem notificações de eventos de interceptação SNMP.
   b. Para habilitar interceptações SNMP para um servidor, selecione a opção **Habilitar**.
   c. Insira o endereço IP do dispositivo host campo **Endereço IP**.
   d. Insira a cadeia de comunidade do dispositivo host no campo **Comunidade**.
   e. Clique em **Salvar configurações**.
4. Configure o módulo de gerenciamento para enviar notificações de eventos ao dispositivo host do Insight RS na guia Eventos.
   a. Clique na guia **Eventos**. Essa tela permite que os administradores definam as notificações de eventos, e-mails ou interceptações SNMP que o módulo de gerenciamento envia para cada evento.
   b. Para cada descrição de evento listada, marque a caixa de seleção **Ativado** para indicar que notificações por e-mail ou interceptações SNMP devem ser enviadas para esse evento. Para habilitar todos os eventos, clique na caixa de seleção **E-mail** e na caixa de seleção **Interceptação SNMP** no topo de cada coluna.
   c. Para cada e-mail e interceptação SNMP habilitada, insira o número de minutos que devem passar entre a ocorrência de uma condição de alerta e o envio da notificação.

   **Observação:** Se o evento desaparecer antes do término do período de atraso, a notificação do evento não será enviada.

   d. Clique em **Salvar configurações**.

### *Definir configurações de firewall e porta*

Para obter uma lista completa de requisitos de firewall e de porta para dispositivos monitorados, consulte o *Informe de Segurança do HP Insight Remote Support*, em: http://www.hp.com/go/insightremotesupport/docs.

## Adicionar credenciais de protocolo e iniciar a detecção

Para detectar seus dispositivos monitorados, conclua as seguintes seções:

### *Criar uma credencial de protocolo SNMPv1 no Insight RS Console*

Se a cadeia da comunidade SNMPv1 do dispositivo estiver definida como `pública` e o modo de acesso da comunidade for `somente leitura`, o Insight RS associará automaticamente um protocolo SNMP ao

seu dispositivo. Se você usar uma cadeia de comunidade diferente ou uma porta não padrão, precisará criar uma credencial de protocolo SNMPv1 no Insight RS Console.

Para configurar o SNMPv1 no Insight RS Console, conclua as seguintes etapas:

1. Em um navegador da Web, faça logon no Insight RS Console.
2. No menu principal, selecione **Detecção** e clique na guia **Credenciais**.
3. Na lista suspensa Selecionar e configurar protocolo, selecione **Simple Network Management Protocol versão 1 (SNMPv1)**.
4. Clique em **Novo**. A caixa de diálogo Nova credencial é exibida.
5. Digite a cadeia de caracteres da comunidade configurada no seu dispositivo.
6. Clique em **Adicionar**.

O Insight RS cria a credencial de protocolo, que é exibida na tabela de credenciais.

### Detectar o dispositivo no Insight RS Console

Para detectar o dispositivo por meio do Insight RS Console, conclua as seguintes etapas:

1. Em um navegador da Web, faça logon no Insight RS Console.
2. No menu principal, selecione **Detecção** e clique na guia **Fontes**.
3. Expanda a seção Endereços IP e adicione o endereço IP do seu dispositivo:
   a. Clique em **Novo**.
   b. Selecione **Endereço único**, **Intervalo de endereços** ou **Lista de endereços**.
   c. Digite os endereços IP dos dispositivos a serem detectados.
   d. Clique em **Adicionar**.
4. Clique em **Iniciar detecção**.

### Verificar o status de detecção e do dispositivo

Para verificar se o dispositivo foi detectado corretamente, conclua as seguintes etapas:

1. Em um navegador da Web, faça logon no Insight RS Console.
2. No menu principal, selecione **Dispositivos** e clique na guia **Resumo do dispositivo**.
3. Verifique se a coluna Status contém um ícone de êxito ().

   Se não houver ícone de êxito, tente descobrir que coluna está com problema e consulte a Ajuda on-line para informações de solução de problemas.

## Verificar a comunicação entre o dispositivo monitorado e o Insight RS

Para verificar a comunicação entre o dispositivo monitorado e o Insight RS, conclua a seguinte seção:

### Enviar uma interceptação de teste

Para enviar uma interceptação de teste, siga estas etapas:

1. Faça logon na interface da web do módulo de gerenciamento UPS.
2. Clique na guia **Configurações**.
3. No menu à esquerda, clique em **Notificações de eventos** e, em seguida, na guia **Interceptações SNMP**.
4. Clique em **Enviar interceptação de teste** para enviar uma interceptação SNMP.
5. Verifique se o Insight Remote Support recebeu a interceptação de teste.

# Configurando módulos de rede UPS

O módulo de rede UPS ((No-break) é um componente opcional opção em várias unidades UPS montáveis em rack e de torre HP, e essas unidades podem ser monitoradas pelo Insight Remote Support nesse módulo.

 **Importante:** Não há suporte para coletas de configuração.

## Atender aos requisitos de configuração

Para configurar módulos de rede UPS de forma que eles sejam monitorados pelo Insight RS, conclua as seguintes seções:

**Tabela 38.2** ***Etapas de configuração do módulo de rede UPS***

| Tarefa | Concluída? |
|---|---|
| Certifique-se de que o Insight RS suporte módulo de rede UPS, verificando o *Notas de Lançamento do HP Insight Remote Support*. | |
| Configurar o SNMP no módulo de rede UPS e defina o dispositivo host como destinatário da armadilha. | |
| Adicione o protocolo SNMP ao Insight RS Console. | |
| Detecte o módulo de rede UPS no Insight RS Console. | |
| Envie um evento de teste para verificar a conectividade entre seu módulo de rede UPS e o Insight RS. | |

## Instalar e configurar o software de comunicação em módulos de rede

Para configurar seus dispositivos monitorados, conclua as seguintes seções:

### Configurar o SNMP

O SNMP pode ser configurado na tela Configurações do SNMP, na interface da web do módulo de rede UPS. A tela Configurações do SNMP permite que um administrador configure o SNMP para computadores que usem o HP Power MIB para solicitar informações do módulo de rede UPS.

Para mais detalhes sobre configurar o SNMP, consulte o *Guia do usuário do módulo de rede UPS HP*.

Para configurar o SNMP, conclua as seguintes etapas:

1. Faça logon na interface da web do módulo de rede UPS.
2. No menu esquerdo, clique em **SNMP**.

3. Selecione a versão do SNMP na lista suspensa Versão SNMP.
4. Preencha os campos adequados.
5. Clique em **Salvar**.
6. Defina o dispositivo host como interface da Web do módulo de rede UPS destinatário da armadilha. A tela Configurações de destinatários de armadilha permite que um administrador configure os aplicativos de gerenciamento de modo a receber armadilhas SNMP do módulo de rede UPS. Aplicativos de gerenciamento SNMP, como o Insight Remote Support, podem receber notificações do módulo de rede UPS.

   Para configurar o dispositivo host como um destinatário de interceptações SNMP, conclua as seguintes etapas:

   a. No menu esquerdo, clique em **Aplicativos notificados** e em **Adicionar destinatário de armadilha**. Configure até três aplicativos para receber interceptações SNMP do Módulo de rede UPS.

b. Digite o nome do aplicativo, como Insight RS, no campo **Nome do aplicativo**. A HP recomenda adicionar "SNMP" ou "Armadilha" ao nome, para monitoramento fácil.

c. Digite o nome de host ou endereço IP do servidor de gerenciamento em que o aplicativo está em execução, no campo **Nome de host ou endereço IP**.

d. Selecione a versão do SNMP na lista suspensa **Protocolo**.

e. Se você tiver selecionado SNMPv1, digite a cadeia de caracteres de comunidade no campo **Comunidade da armadilha**.

f. Marque a caixa de verificação do MIB apropriado:

   - **HP MIB (cpqpower.mib)**—O HP Power MIB
   - **IETF MIB (RFC1628)**—Um UPS MIB padrão

g. Clique em **Salvar**. As informações de aplicativo aparecem na tela Aplicativos notificados.

## *Definir configurações de firewall e porta*

Para obter uma lista completa de requisitos de firewall e de porta para dispositivos monitorados, consulte o *Informe de Segurança do HP Insight Remote Support*, em: http://www.hp.com/go/insightremotesupport/docs.

# Adicionar credenciais de protocolo e iniciar a detecção

Para detectar seus dispositivos monitorados, conclua as seguintes seções:

## *Criar uma credencial de protocolo SNMPv1 no Insight RS Console*

Se a cadeia da comunidade SNMPv1 do dispositivo estiver definida como `pública` e o modo de acesso da comunidade for `somente leitura`, o Insight RS associará automaticamente um protocolo SNMP ao seu dispositivo. Se você usar uma cadeia de comunidade diferente ou uma porta não padrão, precisará criar uma credencial de protocolo SNMPv1 no Insight RS Console.

Para configurar o SNMPv1 no Insight RS Console, conclua as seguintes etapas:

1. Em um navegador da Web, faça logon no Insight RS Console.
2. No menu principal, selecione **Detecção** e clique na guia **Credenciais**.

3. Na lista suspensa Selecionar e configurar protocolo, selecione **Simple Network Management Protocol versão 1 (SNMPv1)**.
4. Clique em **Novo**. A caixa de diálogo Nova credencial é exibida.
5. Digite a cadeia de caracteres da comunidade configurada no seu dispositivo.
6. Clique em **Adicionar**.

O Insight RS cria a credencial de protocolo, que é exibida na tabela de credenciais.

### Detectar o dispositivo no Insight RS Console

Para detectar o dispositivo por meio do Insight RS Console, conclua as seguintes etapas:

1. Em um navegador da Web, faça logon no Insight RS Console.
2. No menu principal, selecione **Detecção** e clique na guia **Fontes**.
3. Expanda a seção Endereços IP e adicione o endereço IP do seu dispositivo:
   a. Clique em **Novo**.
   b. Selecione **Endereço único**, **Intervalo de endereços** ou **Lista de endereços**.
   c. Digite os endereços IP dos dispositivos a serem detectados.
   d. Clique em **Adicionar**.
4. Clique em **Iniciar detecção**.

### Verificar o status de detecção e do dispositivo

Para verificar se o dispositivo foi detectado corretamente, conclua as seguintes etapas:

1. Em um navegador da Web, faça logon no Insight RS Console.
2. No menu principal, selecione **Dispositivos** e clique na guia **Resumo do dispositivo**.
3. Verifique se a coluna Status contém um ícone de êxito ( ).

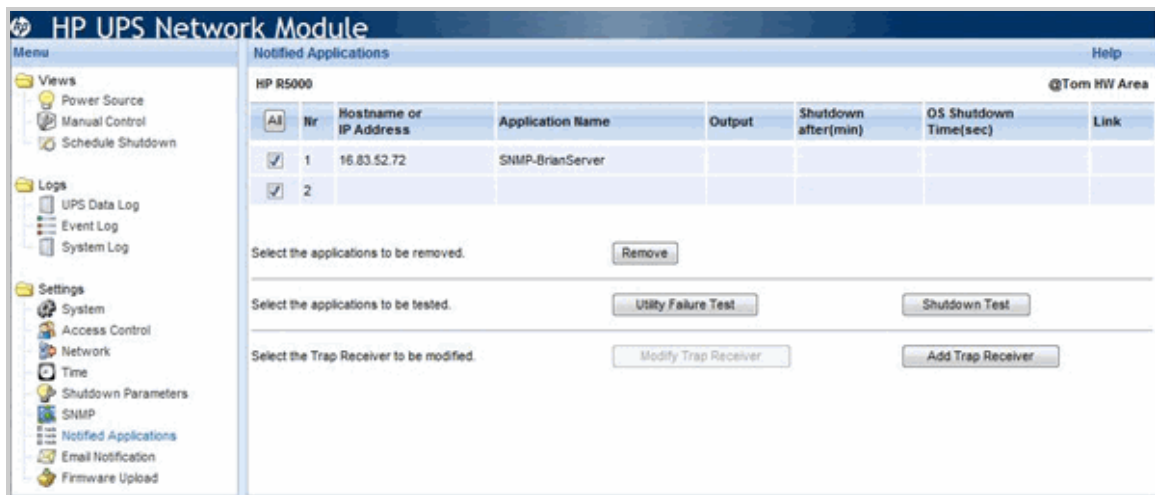
   Se não houver ícone de êxito, tente descobrir que coluna está com problema e consulte a Ajuda on-line para informações de solução de problemas.

## Verificar a comunicação entre o dispositivo monitorado e o Insight RS

Para verificar a comunicação entre o dispositivo monitorado e o Insight RS, conclua a seguinte seção:

### Enviar uma interceptação de teste

Para enviar uma interceptação de teste, siga estas etapas:

1. Faça logon na interface da web do módulo de rede UPS.
2. No menu esquerdo, clique em **Aplicativos notificados** e em **Adicionar destinatário de armadilha**. Até três aplicativos podem ser configurados para receber interceptações SNMP do módulo de rede UPS.

3. Clique em **Teste de falha de utilitário**. O módulo de rede UPS envia uma armadilha de falha de utilitário e envia uma armadilha restaurada de utilitário 30 segundos depois.
4. Verifique se o Insight Remote Support recebeu a interceptação de teste.

# Capítulo 39: Configurar servidores VMware vCenter

O Insight RS pode coletar informações de configuração de máquinas virtuais para o seu ambiente de TI a partir da sua instalação do vCenter. O Insight RS detecta automaticamente qualquer instalação do VMware vCenter quando o servidor ProLiant Windows instalado é detectado, com a condição de que as credenciais de segurança adequadas estejam configuradas.

O Insight RS suporta coletas de guests de máquina virtual vCenter, mas não suporto monitoramento de guests de máquina virtual.

**Observação:** Instalações do vCenter em uma máquina virtual não são suportadas.

A comunicação com uma instalação do vCenter requer a configuração das credenciais de segurança dentro do Insight RS Console. Assim que a detecção ocorre, as informações sobre as máquinas virtuais em qualquer servidor do seu ambiente podem ser coletadas e enviadas automaticamente à HP, de acordo com um agendamento. O cluster do vCenter usa as mesmas informações de garantia e contrato que o servidor ProLiant em que está instalado. Quando servidores ESX e ESXi são detectados, o Insight RS não consegue distinguir que cluster do vCenter os gerencia.

A coleta do vCenter reúne informações sobre os guests da VM e como eles estão configurados no cluster do VMware vCenter. Deve haver um contrato Proactive Care em pelo menos um dos dispositivos ESX ou ESXi que constituem o cluster. Esse é um contrato para todo o ambiente com base no direito de um só servidor, não um direito em relação a cada um dos servidores em que máquinas virtuais estão instaladas.

O cluster vCenter aparece no Insight RS Console com um nome de formulário: `VC@<`*`nomedehost`*`>`.

**Observação:** Apesar de as instalações do vCenter serem visíveis no Insight RS Console, elas não são monitoradas para eventos.

O Insight RS não faz distinção entre vários objetos DataCenter ou entre vários objetos de cluster sendo gerenciados por uma determinada instância do vCenter. O Insight RS 7.4 não tem capacidade hierárquica e, portanto, não pode representar essas construções. Todos os hosts de todos os clusters são adicionados ao Insight RS sem se diferenciarem os vários clusters no qual podem estar configurados.

O Insight RS pode usar a autenticação de tickets CIM em clusters do ESXi gerenciados pelo vSphere, o que oferece as seguintes vantagens:

- Ele permite que o Insight RS se comunique com os hosts ESXi quando eles estão no modo de bloqueio.

  **Importante:** O Insight RS oferece suporte a hosts ESXi no modo de bloqueio quando eles são gerenciados pelo vCenter em uma configuração de cluster. Não há suporte para hosts ESXi autônomos gerenciados pelo vCenter.

- Ele permite que o Insight RS detecte hosts ESXi quando ele detecta o servidor vCenter sem precisar inserir credenciais do WBEM para cada host ESXi; o ticket CIM é usado para as credenciais.

Para habilitar a geração de tickets CIM para dispositivos ESXi, seja no modo de bloqueio ou não, você deve fornecer as credenciais do cluster do VMware vCenter para as tarefas de descoberta (consulte "Criar uma credencial de protocolo de interface de serviço Web do VMWare VirtualCenter no Insight RS Console".) Se qualquer um dos hosts ESXi for um dispositivo ProLiant Gen8, as credenciais RIBCL apropriadas também deverão ser fornecidas antes da detecção.

**Importante:** O recurso de tickets CIM só se aplica ao ESXi, e não aos clusters do ESX. Quando o Insight RS detecta o servidor vCenter, ele também detecta os hosts ESX, mas você deve inserir as credenciais SNMP no Insight RS antes da detecção para que eles sejam monitorados corretamente.

# Atender aos requisitos de configuração

Para configurar servidores VMware vCenter de forma que eles sejam monitorados pelo Insight RS, conclua as seguintes seções:

**Tabela 39.1** ***Etapas de configuração do servidor ProLiant VMware vCenter***

| Tarefa | Concluída? |
|---|---|
| Certifique-se de que o Insight RS suporte seu servidor ProLiant VMware ESX, verificando o *Notas de Lançamento do HP Insight Remote Support*. | |
| Adicione credenciais de protocolo VMware vCenter no Insight RS Console. | |
| Detecte o servidor ProLiant vCenter no Insight RS Console. | |
| Verifique o status do servidor ProLiant VMware ESX no Insight RS Console. | |

# Adicionar credenciais de protocolo e iniciar a detecção

Para detectar seus dispositivos monitorados, conclua as seguintes seções:

## Criar uma credencial de protocolo de interface de serviço Web do VMWare VirtualCenter no Insight RS Console

Para o vCenter ser detectado, você precisa adicionar as credenciais que você usa para fazer login no vCenter. Se essas credenciais não forem adicionadas, o cluster do vCenter não será detectado. Adicionar essa credencial permite a geração de tickets de CIM para dispositivos ESXi, seja no modo de bloqueio ou não.

**Importante:** Se qualquer um dos hosts ESXi for um dispositivo ProLiant Gen8, as credenciais RIBCL apropriadas também deverão ser fornecidas antes da detecção.

Para configurar a interface de serviço Web do VMWare VirtualCenter no Insight RS Console, conclua as seguintes etapas:

1. Faça logon no Insight RS Console.
2. No menu principal, selecione **Detecção** e clique na guia **Credenciais**.

3. Na lista suspensa **Selecionar e configurar protocolo**, selecione **Interface de serviço Web do VMWare VirtualCenter**.
4. Clique em **Novo**. A caixa de diálogo Nova credencial é exibida.
5. Digite o nome de usuário e senha que você usa para fazer logon no vCenter.
6. Clique em **Adicionar**.

# Detectar o servidor ProLiant vCenter no Insight RS Console

Para detectar o servidor ProLiant vCenter por meio do Insight RS Console, conclua as seguintes etapas:

1. Em um navegador da Web, faça logon no Insight RS Console.
2. No menu principal, selecione **Detecção** e clique na guia **Fontes**.
3. Expanda a seção Endereços IP e adicione o endereço IP do seu dispositivo:
   a. Clique em **Novo**.
   b. Selecione **Endereço único**, **Intervalo de endereços** ou **Lista de endereços**.
   c. Digite os endereços IP dos dispositivos a serem detectados. Use o endereço IP do servidor ProLiant em que o vCenter está instalado e, enquanto você tiver credenciais do vCenter configuradas no Insight RS Console, o vCenter também será detectado.
   d. Clique em **Adicionar**.
4. Clique em **Iniciar detecção**.

**Observação:** A detecção do vCenter faz com que os dispositivos ESX e ESXi que ele gerencia sejam detectados quando as credenciais adequadas são fornecidas. Para o ESXi, as credenciais adequadas podem ser o WBEM ou o ticket CIM do vCenter. Certifique-se de que os dispositivos ESX e ESXi tenham as credenciais adequadas configuradas.

# Verificar o status do servidor ProLiant vCenter no Insight RS Console

Para verificar se o dispositivo foi detectado corretamente, conclua as seguintes etapas:

1. Em um navegador da Web, faça logon no Insight RS Console.
2. No menu principal, selecione **Dispositivos** e clique na guia **Resumo do dispositivo**.
3. Verifique se a coluna Status contém um ícone de êxito ().

   Se não houver ícone de êxito, tente descobrir que coluna está com problema e consulte a Ajuda on-line para informações de solução de problemas.

# Verificar a comunicação entre o dispositivo monitorado e o Insight RS

Para verificar a comunicação entre o dispositivo monitorado e o Insight RS, conclua a seguinte seção:

## Verificar coletas no Insight RS Console

Coletas não são executadas automaticamente depois da descoberta. A HP recomenda que você execute uma coleta manualmente após a descoberta completa para verificar a conectividade. Execute o cronograma de coleta manualmente na guia Serviços de coleta → Agendamentos de coleta. Para obter mais informações sobre como agendar coletas, consulte a Ajuda do Insight RS.

Verifique se essa coleta foi bem-sucedida na guia Serviços de coleta → Resultados da coleta básica do Insight RS Console.

1. Faça logon no Insight RS Console.
2. No menu principal, selecione **Serviços de coleta** e depois clique na guia **Resultados da coleta básica**.
3. Expanda a seção Coleta do servidor VMware vCenter.
4. Localize a entrada referente ao seu dispositivo e verifique a coluna Resultado. Se a coleta tiver sido bem-sucedida, um ícone de êxito será exibido ( ). Se ocorrer uma falha, um ícone de erro será exibido ( ).

# Glossário

## A

**agendamentos de coleta**

A frequência na qual coletas são executadas. O agendamento é configurável no Console do Insight RS.

**Agentless Management Service (AMS)**

O iLO 4 Agentless Management usa comunicação fora de banda para aumentar a segurança e a estabilidade. Com o Agentless Management, opções de geração de alertas e monitoramento da integridade estão incorporadas ao sistema, entrando em ação no momento em que um cabo de alimentação é conectado ao servidor. Esse recurso funciona no hardware do iLO, independentemente do sistema operacional e do processador. O AMS instalado separadamente coleta dados adicionais do sistema operacional.

**Assistente de configuração de dispositivo host**

Telas passo a passo que ajudam os usuários com a configuração inicial de seus dispositivos host.

**Assistente de configuração de dispositivo monitorado**

Telas passo a passo que ajudam os usuários a detectar dispositivos em seus ambientes a serem monitorados. Os usuários especificam o intervalo de dispositivos a serem detectados e as credenciais correspondentes.

## B

**Base de Informações de Gerenciamento (MIB)**

A especificação de dados para transmitir informações usando o protocolo SNMP. Um HP MIB também é um banco de dados de objetos gerenciados acessados por protocolos de gerenciamento de rede.

## C

**caso de fluxo de trabalho**

A obrigação específica da HP de enviar uma peça de substituição para uma peça com problemas do cliente.

**CDID**

Consulte ID de entrega personalizada.

**Centralized Management Console (CMC)**

O CMC é usado para configurar e gerenciar os sistemas de armazenamento P4000.

**CLIQ**

Termo legado da interface de linha de comando LeftHand OS. Veja P4000 CLI.

**cluster**

Cluster é um grupo de nós de armazenamento que cria o pool de armazenamento a partir do qual você cria os volumes.

**coleta de configuração**

O HP Insight Remote Support usa o termo coleta de configuração em referência a dados coletados de um dispositivo monitorado. Esses dados são enviados à HP para uma análise proativa.

**coletas**

O termo do HP SIM para sistema de agrupamento ou pesquisas de eventos. Enquanto o HP SIM usa o termo coleta em referência a um grupo de dispositivos monitorados, o Insight Remote Support usa o termo coleta de configuração em referência a dados coletados de um dispositivo monitorado. Esses dados são enviados à HP para uma análise proativa.

## D

**descoberta**

Um recurso dentro de um aplicativo de gerenciamento que localiza e identifica objetos de rede. Em aplicativos de gerenciamento da HP, a descoberta encontra e identifica todos os dispositivos em um intervalo de rede específico.

**direito**

O processo de autorizar uma solicitação para suporte com base no conteúdo dos contratos de garantia ou suporte mantidos pelo cliente, normalmente com relação a um Objeto de serviço (OOS) específico, como um componente de hardware ou software. Seu nível de direito é determinado pelo seu contrato de Suporte HP. Entre em contato com a Equipe de Contas HP para mais detalhes.

**Dispositivo host**

O dispositivo host é um servidor ProLiant compatível com Windows que hospeda o software Insight Remote Support. Quando usado com o HP Systems Insight Manager, o dispositivo host pode agir como um Servidor de Gerenciamento Central (CMS).

**dispositivo monitorado**

Qualquer dispositivo monitorado pelo HP Insight Remote Support, como servidores, sistemas de armazenamento e switches. Para monitorar um dispositivo, algum tipo de protocolo de gerenciamento (por exemplo, SNMP ou WBEM) deve estar presente no dispositivo.

## E

**Enterprise Virtual Array (EVA)**

EVA é uma solução de armazenamento virtual em RAID de alto desempenho, alta capacidade e alta disponibilidade para ambientes corporativos avançados.

**Event Log Monitoring Collector (ELMC)**

O ELMC fornece detecção de condições de erro no registro de eventos e comunica esses eventos ao Insight RS.

**evento**

Um termo geral para todos os tipos de notificações de um processo a outro.

**evento de hardware**

Um tipo específico de evento que sugere que um componente de hardware específico pode estar com problemas. Os eventos de hardware podem resultar em um evento de serviço.

**evento de serviço**

O Insight RS monitora o ambiente de hardware do cliente em busca de eventos de serviço que exigem ação do cliente ou do provedor de serviços (Parceiro distribuidor da HP e/ou equipe de serviços da HP). A maior parte dos eventos de serviço acionáveis requer a substituição de uma FRU (Unidade substituível em campo) ou de uma CRU (Unidade substituível pelo cliente) com defeito no hardware monitorado. Eventos não acionáveis são excluídos, e os eventos de serviço acionáveis são encaminhados à HP. O Insight RS monitora o hardware em busca de falhas permanentes em um componente importante no hardware, como CPU, disco, memória e fonte de alimentação, e essas falhas acionarão uma comunicação de evento de serviço com a HP. Além disso, o Insight RS monitora o hardware em busca de erros temporários e, em alguns casos, quando o número desses erros excede um limite específico, um evento é enviado à HP. Detalhes adicionais sobre o que pode ser classificado como um evento de serviço acionável são considerados informações confidenciais da HP.

## G

### grupo de gerenciamento

Conjunto de um ou mais nós de armazenamento que serve de recipiente para você fazer cluster de nós de armazenamento e criar volumes para armazenamento.

### grupos de dispositivos

Grupos configuráveis de dispositivos no Console do Insight RS que ajuda os usuários a organizar os dispositivos em seu ambiente.

## H

### Health Check (Verificação de integridade)

O utilitário Health Check (Verificação de integridade) da LeftHand Networks é usado para enviar informações de arquivo de registro de monitoramento de locais do cliente para a LeftHand Networks para solução de problemas e monitoramento proativo da integridade. Veja Service Console.

### HP Passport (HPP)

O serviço de acesso simples HP Passport lhe permite usar a ID e a senha de usuário de sua escolha para acessar todos os sites preparados para HP Passport.

## I

### ID de entrega personalizada

A ID de entrega personalizada é um campo de texto livre que pode ser preenchido individualmente para cada dispositivo monitorado. A menos que um valor específico esteja definido na documentação referente à configuração de um dispositivo em particular, esse campo deve ser deixado em branco. Em algumas circunstâncias muito específicas, esse campo também pode ser preenchido por um Representante da HP, para permitir o tratamento/encaminhamento personalizado de incidentes relatados. Nesses casos, o campo deve ser preenchido com um valor único associado ao tratamento personalizado que é necessário. A determinação do valor exclusivo deve ser feita pelo Representante da HP trabalhando com o TS da equipe de automação HP responsável por definir as personalizações. A falha em seguir essa orientação pode resultar em relatórios de incidentes tratados incorretamente.

### identificação

Um aspecto do processo de descoberta que identifica o protocolo de gerenciamento e o tipo do sistema.

### iLO

Integrated Lights-Out. Tecnologia incorporada de gerenciamento de servidores que oferece um gerenciamento remoto baseado na Web que está sempre disponível.

### iLO Remote Insight Board Command Language (RIBCL)

Protocolo de comunicação necessário para o Insight Remote Support se comunicar com servidores ProLiant Gen8.

### Insight Online

O Insight Online fornece acesso direcionado, personalizado e seguro para dar suporte aos dispositivos no seu ambiente de IT. Ele está integrado ao Centro de suporte HP para o seu pessoal de IT, responsável por implantar, gerenciar e dar suporte a sistemas, e também para Parceiros distribuidores autorizado da HP, que dão suporte à sua infraestrutura de IT. O Insight Online pode descobrir automaticamente dispositivos monitorados remotamente pela HP (requer o Insight Remote Support 7.0 ou posterior). Dependendo do seu modelo de suporte, você ou seu Parceiro distribuidor autorizado da HP pode organizar facilmente seus dispositivos em grupos e ter a flexibilidade de realizar com eficiência o monitoramento, o controle e a manutenção dos seus dispositivos da HP.

**Insight Remote Support**

O HP Insight Remote Support fornece monitoramento remoto proativo, diagnóstico e solução de problemas para ajudar a melhorar a disponibilidade de servidores e sistemas de armazenamento HP suportados no seu data center. O HP Insight Remote Support reduz os custos e a complexidade pelo suporte dos sistemas. O HP Insight Remote Support comunica com segurança informações sobre incidentes de hardware ao datacenter da HP através do seu firewall e/ou proxy da Web para fins de suporte reativo. Além disso, com base no contrato de suporte, as informações do sistema podem ser coletadas para uma análise e um serviço proativo.

**Insight RS Console**

A interface de usuário do Insight Remote Support instalada no Dispositivo Host.

**Insight RSA**

Insight Remote Support Advanced. Versão anterior do Insight Remote Support que se integra ao HP SIM para fornecer monitoramento pró-ativo remoto, diagnósticos e solução de problemas de dispositivos.

**integridade do sistema**

O status de integridade é um status completo de todas as fontes de status (que podem ser SNMP, WBEM e HTTP) com o status mais importante sendo exibido.

**Interceptação SNMP**

Evento assíncrono gerado por um agente SNMP que o sistema usa para comunicar uma falha.

## N

**nó virtual**

O P4000 Virtual SAN Appliance usa unidades cativas de disco de servidor para criar uma SAN iSCSI virtual que consiste de nós virtuais que criam o pool de armazenamento a partir do qual volumes virtualizados são criados. O nó virtual pode ser detectado e gerenciado da mesma maneira que o nó de armazenamento físico.

## P

**P4000 CLI**

A P4000 CLI é a interface da linha de comando usada para fazer interface com os sistemas de armazenamento P4000 a partir do dispositivo host. A P4000 CLI é instalada com o Insight Remote Support. Observe que, por vezes, a P4000 CLI é chamada de cliq, que é o nome do comando usado dentro da P4000 CLI.

**Parceiro de serviço autorizado da HP**

Parceiros de canal que fornecem serviços e/ou serviço de instalação em nome da HP.

**protocolo de gerenciamento**

Um conjunto de protocolos, como WBEM, HTTP ou SNMP, usado para estabelecer comunicação com sistemas descobertos.

## R

**Revendedor/distribuidor autorizado da HP**

Parceiros de canal que vendem hardware e serviços.

**RIBCL**

Consulte iLO Remote Insight Board Command Language.

## S

**Service Console**

O Service Console é o software legado que habilitou suporte remoto a hardware e software para os sistemas de armazenamento P4000. Agora essa funcionalidade é fornecida pelo Insight Remote Support. Veja Health Check (Integridade do sistema).

**Serviços HP Care Pack**

Os HP Care Packs podem ser adquiridos com os produtos e serviços da HP para atualizar ou ampliar as garantias-padrão com os pacotes de suporte aprimorados. Eles reduzem os riscos de paralisação, com níveis de suporte do básico ao avançado. Após o encerramento da garantia original, muitos produtos contam com serviços HP Care Pack pós-garantia.

**Servidor de Gerenciamento Central (CMS)**

O CMS é um sistema no domínio de gerenciamento que executa o software HP Systems Insight Manager. Todas as operações centrais do HP Systems Insight Manager são iniciadas a partir desse sistema.

**Simple Network Management Protocol (SNMP)**

Um dos protocolos de gerenciamento suportados pelo Insight Remote Support. Protocolo de gerenciamento tradicional usado amplamente pelos sistemas de rede e pela maioria dos servidores. MIB-2 é a informação-padrão disponível consistentemente em todos os fornecedores.

**Sistemas Qualificados para o Remote Support**

Sistemas que são qualificados para o Remote Support e que, quando habilitados, enviarão eventos ao Centro de Suporte HP para solução de incidentes. Os sistemas devem também ter direito ao Remote Support. Caso contrário, os eventos enviados serão fechados. Você pode verificar se um sistema qualificado é realmente suportado usando a Verificação de Direito do Remote Support.

**Storage Area Network (SAN)**

A SAN é uma rede composta por dispositivos de armazenamento e iniciadores que armazenam e recuperam informações nesses dispositivos, incluindo a infraestrutura de comunicação. Em grandes corporações, uma SAN conecta vários servidores a um pool centralizado de armazenamento em disco. Em comparação com o gerenciamentpo de centenas de servidores, cada um com seus próprios discos, as SANs aprimoram a administração do sistema.

**Storage Management Server (SMS)**

Um sistema no qual o software HP Enterprise Virtual Array (EVA) é instalado, incluindo o HP P6000 Command View e o HP Replication Solutions Manager, se utilizados. É um servidor de gerenciamento dedicado que executa o software de gerenciamento EVA de forma exclusiva.

**System Fault Management (SFM ou SysFaultMgmt)**

O SFM é a solução de gerenciamento de falhas do HP-UX que implementa padrões WBEM. O SFM se integra a outros aplicativos de gerenciamento, como HP SIM, HP SMH e outros clientes com base no WBEM.

**System Management Homepage (SMH)**

A System Management Homepage (SMH) é uma interface baseada na Web que consolida e simplifica o gerenciamento de sistema único para servidores HP nos sistemas operacionais HP-UX, Linux e Windows.

**Systems Insight Manager (SIM)**

O SIM é uma plataforma unificada de gerenciamento de armazenamento e servidores. A partir de um único console de gerenciamento, os administradores podem gerenciar seu ambiente completo de armazenamento e servidor HP com um conjunto de ferramentas de gerenciamento seguro.

## V

**Verificação de Direito do Remote Support (RSEC)**

A RSEC é uma verificação relacionada ao armazenamento de dados de direito da HP para o status de obrigação atual de um determinado sistema. A janela Direito exibe

os resultados da Verificação de Direito do Remote Support.

**volume**

Uma entidade lógica composta de armazenamento em um ou mais nós de armazenamento. Pode ser usado como armazenamento de dados brutos ou pode ser formatado com um sistema de arquivos e usado por um host ou servidor de arquivos.

## W

**Web-Based Enterprise Management (WBEM)**

Essa iniciativa do setor fornece gerenciamento de sistemas, redes, usuários e aplicativos por vários ambientes de fornecedores. O WBEM simplifica o gerenciamento do sistema, fornecendo melhor acesso a dados de software e hardware que pode ser lido por aplicativos cliente WBEM.

**Windows Management Instrumentation (WMI)**

Implementação da Microsoft do Gerenciamento Corporativo Baseado na Web (WBEM).

# Índice